PRIVACY, CONFIDENTIALITY AND SECURITY IN A CANADIAN ELECTRONIC FUNDS TRANSFER SYSTEM

Working Paper #5

Professor David H. Flaherty

PRIVACY, CONFIDENTIALITY AND SECURITY IN A CANADIAN ELECTRONIC FUNDS TRANSFER SYSTEM

Working Paper #5

Professor David H. Flaherty

This background paper is one of a series which has been developed in connection with a research project directed by Professor Richard H. McLaren. It is directed at identifying specific issues within a designated topic. The research project was designed to identify the "Policy and Legislative Responses to Electronic Funds Transfer" from a provincial perspective.

TABLE OF CONTENTS

I. INTRODUCTION

This Working Paper will discuss the challenges posed for personal privacy and the confidentiality and security of personal data by the gradual implementation of an electronic funds transfer system (EFT) in Canada. The focus will be on the various problems presented by EFT, how they are being handled in current services and practices of financial institutions, and what solutions and regulatory models are needed for protective purposes. The working definitions employed herein are simple. Although the literature on privacy is growing rapidly, the problem of defining the term remains an elusive one. Privacy refers generally to a person's desire to be left alone and to control the dissemination of information concerning him or her.[1] Confidentiality refers to the status of data or personal information pertaining to a particular person; concern for confidentiality is an aspect of protecting personal privacy. The issue of security refers to particular measures, often physical in character, which custodians take to protect the confidentiality of personal data. The Association of Data Processing Service Organizations (ADAPSO) has summarized the issue as follows in its policy on data privacy and security: "Privacy is a social issue which involves the question of what data should be collected, stored and disseminated. Security deals with the procedures to assure confidentiality; i.e., the protection of information from improper disclosure, modification, or destruction."[2]

It will obviously be necessary to provide adequate safeguards against possible misuses of personal information in an EFT system. Yet, whatever analytical categories are used to catalog potential abuses, an EFT system is simply another in a long list of technological innovations that have escalated the level of challenge to personal privacy since the Second World War. Individuals are no longer in a position where they can rely solely on their own efforts to protect their personal

privacy. Viewing EFT even in a modest historical context suggests that the resultant problems for privacy it presents are as amenable to control and regulation as any other recent technological innovations in computerized data handling. Yet past experience with various technical innovations also suggests that proponents of EFT have been and are much more concerned about its technological difficulties and commercial prospects than the challenges the system presents for personal privacy. Full-scale consumer acceptance of EFT in its various forms will depend heavily on reducing individual anxieties about potential threats to personal privacy. Even if a strict system of regulatory and physical controls to protect confidentiality is built into the elements of an EFT system, the common fears associated with computers will still remain.

During the last decade concern for personal privacy has surfaced as one of the leading half dozen issues arousing citizens of modern industrial societies. The issue of privacy serves as a rallying point for a wide variety of anxieties generated by the growth of central bureaucratic governments and multi-national corporations. The "Privacy Lobby" has become very powerful in recent years, as evidenced by the introduction of data protection laws in the United States, Sweden, Canada, the Federal Republic of Germany, and other countries. The gradual implementation of EFT is paralleling this movement toward data protection as the main government effort to protect personal privacy.

The final report of the Privacy Protection Study Commission in the United States in 1977 listed the following objectives for national policy making in an information society: minimizing intrusiveness in data collection; maximizing fairness in recording and storing data; and legitimizing expectations of confidentiality for data.[3] Comparable goals will be crucial to protect privacy and related values in the introduction of an

operational system of EFT in North America. It is indeed fortunate that EFT is merely the latest in a series of technological innovations: modern societies have learned a great deal about how to cope with and regulate such novelties in the interests of the citizenry at large. This Working Paper will discuss the characteristics of an EFT system that should help to allay the concerns of Canadian consumers and civil libertarians. The goal will be to set forth various general measures for regulation of a Canadian EFT system in the interests of protecting the personal privacy of citizens of Ontario.

II. THE CHALLENGE TO PRIVACY, CONFIDENTIALITY, AND SECURITY

II.a. The General Concern

It is not difficult to articulate general concern about the challenge to privacy and confidentiality of an EFT system, since most popular writing has focused on these types of worries. Although this Working Paper will attempt to move beyond this level of sensitivity to an identification of real problems and solutions, it is initially useful to focus on concern at the general level. The late United States Supreme Court Justice William O. Douglas articulated a form of popular anxiety in his dissenting opinion in California Bankers Association v. Shultz:

> In a sense a person is defined by the checks he writes. By examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum. These are all tied to one's social security number; and now that we have the data banks, these other items will enrich that storehouse and make it possible for a bureaucrat - by pushing one button - to get in an instant the names of the 190 million Americans who are subversives or potential and likely candidates.[4]

Justice Douglas's vivid language raises the spectre of the challenge to the confidentiality of EFT data posed by record-keepers, governments, and third parties.

The information in an operating EFT system has potential value for personal embarrassment, commercial uses, and political surveillance.[5] Thus, the need for the verification of identity raises the whole issue of personal identification numbers (PIN), including the threat of uniform EFT identity cards and data banks for identity verification. This has a direct tie-in to the hostile debates in North America about government requirements for social security numbers and social insurance numbers.[6]

At a more manageable level than crudely articulated popular fears, the development of EFT poses considerable practical problems

for the protection of the interests of consumers. In the United States the National Commission on Electronic Fund Transfers (NCEFT) was required by law to investigate "the need to afford maximum user and consumer rights to privacy and confidentiality."[7] In its first major interim report the Commission concluded that the interests of consumers were "the most critical factor in all its recommendations."[8] It has thus become a commonplace of the literature on EFT to suggest that consumer issues, especially concern for privacy and confidentiality, are the most critical ones in terms of the ultimate implementation of national EFT systems.[9]

II.b. The Challenge of Computerized Banking

The general public has an extraordinary love-hate relationship with computers. Most persons know little about computers, yet use them widely and fear them greatly. In the last decade the threat posed by computers to one human value or another has been a popular theme in magazine writing.[10] Thus a certain amount of the expressed concern about the fate of personal privacy with the advent of EFT derives from the usual exaggerated fear of computers. Almost every new mechanization of information-handling brings forth both imaginative and realistic descriptions of the potential threat to human rights and civil liberties. In this context it is worthwhile reflecting how few persons today seem overtly to worry about the confidentiality of data about them in the Master Charge or Visa credit card systems. Herbert A. Simon, who is professor of computer science and psychology at Carnegie-Mellon University, has observed that "making the computer the villain in the invasion of privacy or encroachment on civil liberties simply diverts attention from the real dangers. Computer data banks can and must be given the highest degree of protection from abuse."[11] Computers need to be controlled and regulated in such a manner that important societal benefits are not lost.

The general public fear of computers leads directly to concern about the gradual implementation of computerized banking in North America, even though "the majority of EFT computer systems used

today are operated in the 'off-line' mode, where there is no direct telephone line between the terminal and the host computer."[12] But it is obvious that EFT systems are well suited to on-line data processing, where there will be direct communication over telephone lines and other electronic modes. Public concerns about on-line banking seem more realistic if they begin with an awareness of the type of on-line banking already in operation in Japan, for example. The largest Japanese bank has a national system of on-line banking with three large-scale computers, seven hundred mini-computers, and four thousand terminals. There are ten thousand cash dispensers in the entire country, almost all of them on-line. Two hundred cash dispensers installed at geographically dispersed public places allow depositors to withdraw cash from any of fifty-four subscribing banks. The on-line exchange system of all banks in Japan, known as Zengin, has a common network shared by 7,500 branches of 90 banks.[13]

Although mechanized banking is not as developed in North America as in Japan, and some Western European nations, there are enough examples of on-line banking in Canada to permit problems to be identified. The basic point is that many potential threats to personal privacy inherent in EFT already exist in a largely paper-based banking system. Mechanized banking is spreading very rapidly in Canada. More than 1,250 caisses populaires across the province of Quebec are linked in a well-developed on-line system. The relatively large size and dispersion of the Canadian chartered banks in comparison to their American counterparts further increases the scope for mechanization in Canada. The Royal Bank of Canada, for example, has over 1,500 branch offices, 6 Canadian data processing facilities, and at least 100 computerized systems.[14] The Bank of Montreal has passed the half way mark in its program of branch mechanization, "providing for automatic handling of transactions associated with deposit accounting services."[15] At the end of 1977 approximately 650 branches of the Bank of Montreal in Ontario, Quebec, and the West were functioning in an on-line mode.

It is arguable that the concentration of almost 40 percent of chartered bank branches in Ontario, coupled with the current concentration of on-line banking terminals in the same province, increases the threat of computerized banking to the privacy of Ontario residents.[16] Problems are more likely to develop first in Ontario than in other provinces because of the attractiveness of the Ontario market as a locale for computerized banking and a target for EFT-related banking services, such as Automated Teller Machines (ATMs).

The spread of on-line banking is a fundamental step in the development of a national EFT system. It has definite benefits for consumers. The Niagara Credit Union, for example, plans to install an on-line banking service, which will provide it with instant access to member accounts for teller services.[17] But it is worth remembering that this common characteristic of "instant access" can also be used for less than desirable purposes. The Bank of Montreal publishes a brochure on how the computer improves banking services. It describes how the system "gives you, through your teller, immediate access to up-to-the-minute information on your account .... However, if instead you ask to see your account, it will type out everything that's happened on your account since your last statement, including your up-to-the-minute balance. The same sort of thing happens on your savings account when you ask for your balance or want your passbook up-dated." It requires little imagination to recognize that this feature can also be abused at the expense of personal privacy. The Bank of Montreal brochure in fact attempts to answer the question of "how you are protected" with the following simple statement: "The system improves confidentiality. Only a bonded bank officer using special codes can gain access to the computer system each day. After hours, the lines are shut down." This assertion is at least debatable. Computerization does produce greater control over the confidentiality of data when manual files are replaced, but the Bank of Montreal system in fact produces a series of print-outs on individual accounts

that are available to any bank employee like manual files.

The potential for abuse of computerized banking will become much greater when branches of Canadian chartered banks are in fact completely linked on a coast-to-coast on-line network. The challenge will be further increased if and when a series of national Point of Sale (POS) networks are developed in Canada. Competitive considerations suggest that there will never be a single network. Although there are currently no POS terminals in use in Canada in a strict sense, the time is ripe to anticipate potential issues.[18] In fact, Steinberg's grocery chain is using an automated scanner system for checking out groceries, which it regards as a POS system. The data obtained from reading universal product codes are automatically centralized for billing, inventory control, and re-ordering. The issues associated with Automated Teller Machines (ATMs) will no doubt surface more quickly as a basic problem as more and more ATMs function in an on-line mode.

The Banque Canadienne Nationale has described how its on-line banking system enjoys "the security inherent in a complete in-house operation backed up by a bank-oriented EDP staff."[19] A contrasting situation may exist for financial institutions using a product such as the IBM 3614 ATM, which is supported in an on-line mode by IBM data processing services. Such reliance on computer service bureaus may increase the problem of protecting the confidentiality of customer information, since moving data between outside computers and financial institutions creates a level of risk. Even with the support of IBM data processing service, the main information on customers and their accounts remains in the files of the financial institution, so that financial "data must be transmitted back and forth between the IBM service bureau computer and the central files."[20] For this reason, the IBM ATMs encrypt basic financial data in transit. The issue of confidentiality may become even more acute when a computer service bureau maintains all of the mechanized data files for small banks and trust companies.[21] A single computer

may contain personal data from a wide range of clients, further increasing the risk of unauthorized access.

II.c. The Challenge of Data Collection and Transmission

The gradual implementation of EFT challenges the common assertion that "there is no existing mechanism for building an automatic cumulative record of all of a person's transactions of all kinds."[22] It is generally agreed that the mechanization of banking procedures, which may ultimately lead to a fully-developed EFT system, involves the creation of massive centralized personal transaction files. This will increase both the scope of information gathering and its accessibility. The American Privacy Protection Study Commission identified the new type of data developed in an EFT environment: "'Transaction' or 'event-related' data, as they are called, are a new phenomenon inasmuch as the individual actions that generate them have not traditionally generated any kind of permanent record. Moreover, the individual is often unaware that he is generating those machine-readable trails that provide an increasingly more detailed profile of his life."[23]

EFT services also make possible the creation and use of new systems of records. A Virginia bank reported in 1976 that it was developing a computerized customer information service that "will permit it to correlate a customer's use of different services throughout its 137-branch system."[24] This system will identify classes of customers for new services by compiling a synopsis of deposit and loan account information from the customer, credit bureaus, creditors, and the bank's own summary of experience with a customer. Thus even in the early 1970s, the Bank of America, which has been a major innovator in the use of computers, was sceptical about the future of EFT because of the fundamental difficulties of "overcoming public fears about possible invasion of privacy through the creation of centralized personal transaction files."[25]

The implementation of various elements in an EFT system will make more financial transaction information available. It is not simply a case of mechanizing information already available in manual files at financial institutions. The amount of information that can be merged through an EFT system creates a totally new level of risk to human values; it will not be enough merely to extend current protective practices. The American National Commission on Electronic Fund Transfers (NCEFT) determined that the information captured in an EFT transaction might include name, address, account number, account balance, debit and credit amounts, debit and credit payees or payors, location, date, and time of transaction.[26] NCEFT concluded that consumer fears about the use of such data by governments and the private sector are legitimate and genuine. The Commission determined that "present legal safeguards for the privacy of financial transaction information, irrespective of their sufficiency today, are not adequate to deal with threats to privacy that may arise with EFT."[27] In broad terms, these warnings are as applicable to Canada. EFT will generate new kinds of records, increase the amount of information collected, make the data easier to retrieve, and increase the number of institutions with access to the data. Thus an on-line EFT system could be employed to locate individuals at the precise moment when they are using the system.[28]

In the absence of appropriate regulation, the potential uses and abuses of EFT transaction data are limited only by the human imagination. It is currently possible to store and make readily available at least several pages of information on every Canadian citizen. The computerization of financial data makes possible a level of accessibility to data that was too expensive and inconvenient for manual files. Data can be stored for long periods and can be retrieved very quickly.[29] A store using a POS system could be on-line to a full-service bank's central records, "and, possibly, through a switching mechanism, to the records of other banks as well."[30] Although such a system would be designed to

avoid bad credit risks, its implications for privacy are ominous. Various studies of record-keeping in contemporary society suggest that where administrative information is kept, it will be sought and used.[31] In recent years in the United States "the amount of information retained by financial institutions in their ordinary course of business has greatly increased."[32] This increase in recording transactions that were unrecorded in the past has occurred before the major spread of EFT systems and in response to new American legislation such as the Bank Secrecy Act of 1970.

In Canada, financial institutions increasingly use Data Base Management Systems as techniques to build "Customer Information Files," which integrate all information on customers pertaining to accounts and loans.[33] Canadian banks are even now considering the integration of credit card information with other customer data; this is the type of "progress" that computerization makes possible. Such practices increase the prospects of creating a formidable dossier on every member of society, which can be combined "to produce a devastatingly detailed and accurate profile of each member of the society."[34]

In agreeing that EFT will increase the scope of record-keeping, the American Privacy Protection Study Commission added that "there are pressures which could eventually transform EFT systems into generalized information transfer systems."[35] The payment and administrative information generated in an EFT system will have substantial potential for private exploitation and abuse. The CBS television program "Sixty Minutes" conducted an experiment in which a couple's chequing account records for one year were furnished to a private detective for analysis. From the bank records the detective was able to learn the religious affiliation, political and philosophical beliefs, and financial situation of the couple.[36] Other commentators attempting to draw attention to the potential threat of EFT records have produced hypothetical "daily surveillance sheets" on particular individuals, which might be the product of a computer analysis of EFT and similar nationwide databanks.[37]

Studies carried out by the consulting firm of Arthur D. Little Inc. and by the National Commission on Electronic Fund Transfers both suggest the potential use of EFT transaction data for marketing purposes.[38] Such information will be accessible, low-cost, and not previously available; as usual, it can be used for legitimate and detrimental purposes. Many citizens would not appreciate an invitation to take advantage of certain products or services, because an analysis of their financial transactions had indicated that they were likely prospects. The Privacy Protection Study Commission pointed out that "large-scale credit-card systems already monitor frequency of card use and point-of-sale services extend the range of potential surveillance."[39] James B. Rule, an authority on privacy, has written that EFT will "provide a potent new tool for the enforcement of financial obligations."[40] POS can also be used to locate persons. Telecredit Inc., a nationwide independent cheque-guarantee service in the United States, is already deriving revenue from POS by forwarding current addresses of users to its clients.[41] Such practices are a reminder of the necessity to balance various values, including privacy; honest people have an interest in keeping bad debts and prices down, but they are also likely to resent continuous surveillance.

II.d. The Challenge of Information Exchanges and Communication Links

The existence and development of various types of information exchanges and financial networks increases the threat of interception and abuse of personal data. The wiretapping of on-line information networks by means of spoofers or imposter terminals is the most obvious form of interception.[42] Most financial institutions now operate private financial networks over leased lines, but there is a tendency in both the United States and Canada toward public networks.[43] Private leased lines remain susceptible to interception, since they go through exchanges; however it is possible to arrange a completely in-house private network. The greater susceptibility of a public network derives from the reliance

on switching mechanisms and the fact of direct government operation of the system. The literature suggests that private data networks do not appear to threaten the public interest, so much as the potential for government intervention in public networks. For example, 115 subscriber banks in 75 Canadian and American cities use a system known as Bank Wire, which is a private network for the transfer of funds. The computer switches for this system are located in New York and Chicago. Bank Wire II will be operational in 1978.[44] It is a nationwide domestic EFT system owned co-operatively by the banking industry and operated by Payment and Telecommunications Services Corporation. Bank Wire II provides funds transfer services for 195 member banks. The system uses concentrator points in New Jersey, Iowa, and Texas.[45] Presumably, Bank Wire uses various methods to protect the security and confidentiality of communications, yet it remains an example of a private network which has escaped public commentary in large measure. Are the users adequately sensitive to the confidentiality of personal data? The same holds true for existing Automated Clearing Houses (ACHs) in the United States, despite the fact that they seem to anticipate POS networks. ACHs primarily function for the exchange of cheques among various banks. In the United States it is recognized that ACHs already collect and centralize a great deal of information and transfer more than just payment data among institutions. In addition, the Federal Reserve, which operates many ACHs, is now starting to link them across the country.[46]

A fully-developed EFT system will involve a series of remote terminals for the operation of retail POS outlets. This will require cooperation among competing institutions and the establishment of an Automated Clearing House to serve as a common switching and processing centre.[47] An ACH of this type is normally known as a switching centre or switch. A switch means an electronic communication facility which has the ability to receive and transmit on-line data regarding financial transactions between depository and non-depository institutions.[48] Systems of switches would collect

and exchange an enormous amount of information: "Shared systems also require a switch to route messages among participating merchants and depository institutions. The switch might maintain temporary backup records called 'memo files' for control and audit purposes, which are updated for each transaction that flows through the system."[49] In the United States, the NCEFT has expressed considerable opposition to government operation of POS switching systems because of the potential threat to privacy involved. It would be easier for the government to obtain access to personal information under such a system and harder for an individual to defend himself against the government. In connection with POS switches, NCEFT has recommended that the government should play a regulatory role to protect personal privacy and not an operational one.[50] The essential need is for some form of regulation.

For a variety of reasons, the Canadian situation with respect to POS networks seems to be developing in a different manner than in the United States, primarily because of federal government initiatives. It is less clear in Canada that the national government can or will be held at arm's length from an operating POS system. The chartered banks and non-bank deposit-taking institutions in Canada already are linked in a national payment system, which includes a clearing system.[51] Settlement points in the clearing system are operated by the Bank of Canada in ten major cities; the settlement information is telegraphed to Ottawa. This current system is for the clearing of cheques among financial institutions.

In January, 1975, the Government of Canada, led by then Finance Minister John N. Turner, published a document entitled "Towards an Electronic Payments System," The federal government supports a "common user communications network" for the payment system, which should be nationwide, publicly accessible, a shared facility, and have adequate security.[52] It is intended that a national network will be established under the auspices of a

Canadian Payments Association under the forthcoming federal Bank Act. One author calls such a proposal a "national EFT system."[53] Although it seems likely that such a nationwide system would be provided by existing common carriers rather than by a government organization, the various characteristics just outlined suggest that it will be easier for governments to abuse such a system through unauthorized access to personal data. It seems suggestive that a twenty-five page document on EFT in Canada only discussed personal privacy in seven lines on the second-last page.[54] One letter writer reacted as follows: "John Turner's proposed Government-directed national electronic payment system will be a supremely efficient weapon in the arsenal of our present authoritarian regime for manipulating and controlling the populace. When the computerized bureaucracy finally takes over our paycheques and personal accounting we can say goodbye to the last poor tattered shreds of our privacy and freedom."[55] The revelations about the RCMP in 1977-78 lend some credibility to such fears. The essential problem seems to be that the federal government is moving ahead to encourage a national clearing system without sufficient attention, at least in public, to issues of privacy, confidentiality, and security.

The 1976 White Paper on the revision of the Bank Act proposed a Canadian Payments Association Act.[56] It would create a national clearing system to which all deposit institutions would belong. The Payments Association would have its own Board of Directors and be under the inspection of the Inspector General of Banks. The White Paper also expected the creation of a "payment card" for use by individuals in POS terminals. Once again such a proposal did not take overt account of the interests of consumers and civil libertarians.

II.e. The Challenge of Government Surveillance

Increasing computerization of financial transaction information and the creation of national EFT networks present major opportunities

for government surveillance of individuals. This challenge has been recognized in both the popular press and the serious literature on EFT. In Great Britain, critics of plans for a vast computerized payment system charge that government ownership of the system would be "the last straw" on the path to George Orwell's 1984.[57] In response to a widely-circulated article in the popular press, 6,000 Americans wrote critical letters to NCEFT in late 1976: "A majority of writers mentioned invasion of privacy by Government as the basis for their opposition."[58] An American writer identified the government as a leading potential invader of privacy in an EFT system: "Safety approaches in EFT software designs to prevent invasions will be useless against the resources and power of the invaders, as they have been constituted up to now. Can you imagine trying to devise a software-hardware combination that would freeze out the CIA, FBI, and IRS, if they were not stopped in other ways from tapping files?"[59] In 1978, Canadians can no longer argue that such a scenario is only plausible south of the border. The popular Canadian writer Silver Donald Cameron published an article on "The Death of Money" with the subheading: "Will that be cash - or Big Brother? Soon you may have no choice. The computer will know all."[60] The theme of Cameron's article was the substantial increase in the prospects for social control: "The data assembled by the Electronic Payments System could be a source of terrifying power in the wrong hands."[61] A manager of systems development for the Ontario Ministry of Education furnished Cameron with a sensational description of the threat of huge amounts of data stored in an EFT system: "Punch the right buttons, and you can record and recall the movements of anyone in the country, moment by moment, for months and years at a time. I find that terrifying."[62]

In the United States, the NCEFT concluded that "consumers view the Federal Government as a primary threat to the privacy of individual financial transaction information."[63] Although the Commission recommended stricter controls to prevent such abuses, a dissenting member suggested that the Commission had not

sufficiently recognized the threat of using EFT for real time surveillance.[64] James B. Rule has also articulated the potential of EFT as a bureaucratic tool for social control by government or private institutions. EFT has a high system capacity for mass surveillance and control and its introduction "would quickly effect a distinct increase in surveillance capacity."[65] A study of government access to financial records drew the following conclusions:

> The development of an electronic funds transfer system in lieu of current paper check payments will provide more information concerning depositors' transactions and will place the data in a readily accessible and usable form. The ability to retrieve quickly information concerning individuals' payments and receipts creates a specter of computerized searches of thousands of accounts for specified funds transfers. In light of the massive record-keeping of personal financial transactions, unrestricted government access to bank records poses a severe threat to civil liberties and privacy.[66]

In its Hearings on Depository and Lending Institutions, the Privacy Protection Study Commission learned that "informal access to bank records....was a favorite tool of government investigators."[67] A study by the Commission's staff concluded that computerization improves the likelihood of informal access occurring:

> When the banker's records are no longer ledger entries and boxed receipts, but electronic and microfilm files that can be retrieved almost instantly at remote terminals, the cost of retrieval becomes minimal and, thus, the pressure to accede to requests, particularly official ones, becomes greater. When it costs the banker little or nothing to disclose detailed record information, when there are no legal barriers to such disclosure, and when the goodwill of those on whom the banker must rely for cooperation or services, such as law enforcement officers, can be increased, the pressures to disclose become enormous and often insurmountable.[68]

In the United States, financial records have been widely used as a means of political surveillance during the last decade

against such persons as Jane Fonda, Dr. Benjamin Spock, and Dr. Martin Luther King, Jr.[69] The revelations in Canada in 1977-78 concerning the various activities of the security arm of the RCMP suggest that the records of Canadian financial institutions have probably not been immune from informal RCMP scrutiny. The RCMP obtained access to OHIP data in Ontario, despite the fact that the governing statute forbade such a practice. This was also true in connection with RCMP access to National Revenue data.

In the United States the Bank Secrecy Act of 1970 imposed record-keeping requirements on banks for the purposes of law enforcement. The further computerization of banking records through EFT will presumably accelerate this tendency in North America.[70] Even if government access to financial transaction information is fully controlled, financial institutions and the operators of an EFT system are not in a strong position to resist government pressure to use EFT for informal surveillance, since the industry is so heavily regulated by various government agencies.

II.f. The Challenge of Unauthorized Access

The massive collection and exchange of information in computerized banking and EFT systems presents substantial opportunities for unauthorized access to the information by means of fraud and other forms of illicit activity. The NCEFT defined security in EFT "as the protection of financial data in EFT systems against unauthorized and intentional alterations or disclosure to commit fraud."[71] In terms of security, the vulnerable points in an EFT system include the terminals, which are open to impostors, counterfeit cards, and EFT systems personnel; the communication links, which can be wiretapped or otherwise penetrated; and the computers, which are accessible to operators of the system.[72]

Security experts focus on insiders as the major source of

subversion of a computer system. A major IBM study concluded that "studies on fraud and embezzlement involving computers in most cases show an employee is involved - acting either alone or in collusion with others outside the organization. Dishonest people are most likely to misuse the data and functions they have been authorized to use."[73] This group can include programmers, tellers, key-punch operators, and equipment maintenance personnel. Mechanized banking facilitates access by bank personnel to a substantial range of information about customers. In 1977, chartered banks in Canada had 7,252 branches and 145,379 employees.[74]

Preventing penetration of the system by insiders or outsiders is not made any easier when financial institutions use private computer service bureaus. Metropolitan Trust Company,for example, has twelve branches on-line in Toronto, but the main computer is in a service bureau.[75] Customers of service bureaus apparently rely on them to take protective measures. On one occasion a company received a print-out belonging to another customer of the service bureau.[76] In January, 1973, the RCMP broke into a service bureau in Montreal in order to steal computer tapes containing membership information on the Parti Québecois. The RCMP was able to obtain detailed information on the security system at the service bureau from the manufacturer of the particular computer.[77]

The problems of computer fraud in Canada are facilitated by the existence of many common carrier transmission lines used by the banks and operated by such groups as CN/CP and Bell Canada. Although any electronic data network can be penetrated, common carrier transmission lines are particularly easy to intercept.[78] Computer fraud is also difficult to discover, since checking for fraud has normally not been (but should be) part of an auditor's job; many auditors are also unfamiliar with EDP techniques.[79]

NCEFT "found that the vulnerability of EFT systems is easily overstated, and that security can be maintained in an EFT environment."[80] Alan F. Westin and Michael Baker,in their major study

of private and public data banks,asked fifty-five organizations, as well as consultants, for "an instance in which unauthorized access to a computer file of personal data had been obtained in his organization solely through technical means and without inside information or assistance." In the early 1970s, "none of these experts could recall an instance where complete outsiders had, without inside knowledge or aid from a cooperating employee, gained unauthorized access to computerized files to obtain information about individuals contained there."[81] This type of optimistic conclusion may in fact indicate that intrusions remain undetected and that informal access by government agents are not viewed as falling within the scope of this inquiry. The problem of unreported crime may be even greater in the computer field than in general criminal activity. Yet the current literature on computer crime reveals many breaches of allegedly secure systems, including those of financial institutions.[82] The conclusion of a Canadian computer expert seems relevant here: "It is not surprising that it is difficult to cite specific examples of computer fraud because it is a characteristic of this problem that all parties related to a particular fraud have little to gain and much to lose from the publicity. As a result, fully documented cases are rare and in those infrequent instances where information is given to the public, it is often very brief."[83] Whatever the previous record of protecting computers from fraudulent uses, the potential for unauthorized access seems substantially increased with the development of EFT.

At the National Security Conference of Canadian Financial Institutions in Toronto on November 15, 1977, Major Tom Wiley of the RCMP's EDP Section discussed "Security in an Automated Payment System." In his view, an EFT system should protect confidentiality and restrict the flow of personal information. Yet it was his judgment that security is currently haphazard, vulnerability is rampant, and management is passive. Wiley argued that conscientious concern for security at financial institutions requires risk analysis by management and then risk management by outside experts.

II.g. The Interests of Consumers

It is generally recognized that acceptance by consumers will be a crucial issue in the future development of EFT. The potential for consumer resistance is particularly thought to revolve around such issues as privacy, confidentiality, and security.[84] Consumers will have to make a significant decision in balancing the relative benefits and liabilities of EFT.[85] Experience with the operation of a POS network in Iowa suggests that consumers are not adverse to EFT practices: "There, on a daily basis, consumers conveniently deposit funds, withdraw funds, and transfer funds anywhere throughout the state at numerous retail locations."[86] In Canada, the Bank of Montreal claims that its ATM known as "Instabank 724" has won "strong consumer acceptance."[87]

It is of course difficult at this stage to measure the response of Canadian consumers to a developing EFT system, especially in terms of relative concern for privacy, confidentiality, and security. Canadians are demonstrably less overt than Americans in their concern for civil liberties. In the United States, the Bank Administration Institute and the Food Marketing Institute produced a research report on the location of banking services in six supermarkets, including POS terminals, cheque authorization services, and ATMs: "Neither privacy nor security of electronic banking services surfaced as an issue in the focus groups and shopper interviews. When either subject was mentioned, discussions centred on what might happen in the future rather than on specific concerns about, or bad experiences with, existing services."[88] Two recent surveys of consumers' attitudes toward EFT were conducted by the same two groups and also by the Bank Marketing Association: "In both studies, consumers placed more emphasis on convenience than on concerns about security, privacy, and loss of float."[89] Payments System Incorporated of Atlanta, Georgia is doing a new survey of consumers' attitudes toward EFT. The results are due in 1978.[90]

It may be overly optimistic to assume that consumers will in fact have an impact on the development of EFT in North America. While there may be some initial consumer reluctance to allow electronic transfers from their savings and chequing accounts, consumer resistance would probably vanish before a good advertising campaign.[91] Although NCEFT believes that consumers "will determine how EFT will operate," there are similar reasons to doubt the resistance of consumers to a strong marketing strategy."[92] Such prospects seem extremely likely in Canada where the financial institutions are large and powerful and the consumer movement is almost non-existent in comparison to the United States. Another relevant consideration is the relative economic illiteracy of consumers, who do not generally understand their rights and responsibilities in dealing with financial institutions.[93] Canadian consumers no doubt expect confidentiality for their financial transaction information, but it is not at all clear that such expectations are either fulfilled or adequately protected.

The fate of consumers seems to be clear in light of the conclusion of Arthur D. Little Inc. that by 1985 consumers in the United States will be carrying a transaction card as a multi-purpose payment vehicle, for such uses as cheque guarantees, debits, and credits.[94] It is refreshing to read the advice to consumers of Albert A. Foer, a member of NCEFT, who concluded that "consumers should look at EFT with a skeptical eye. Some EFT functions will probably be to their advantage, especially when accompanied by consumer protections that are generally acceptable to most interested parties ... By clarifying and making their interests understood now, consumers can still shape the various EFT systems, relying upon the ultimate weapon of consumer resistance in those areas where sufficient protections are not forthcoming."[95] This good advice is probably not predictive of the future, especially in Canada.

III. PRIVACY, CONFIDENTIALITY, AND SECURITY IN THE CURRENT SERVICES AND PRACTICES OF FINANCIAL INSTITUTIONS

III.a. Concern for Confidentiality

Financial institutions have traditionally expressed strong concern for the confidentiality of customer information, although their situation does not approximate that of national statistical organizations such as the American Bureau of the Census or Statistics Canada, which by law are not permitted to release identifiable data. The aphorism that confidentiality is the lifeblood of the organization applies more to a statistical agency than to a financial institution, since the latter do release information under certain circumstances. American commentators have concluded that the commercial bank's traditional concern for confidentiality justifies a depositor's expectation of privacy:

> Commercial banks have rigorously maintained the confidentiality of checking account transactions. Generally information is released to private parties only upon consent of the depositor and is confined to credit information. Raw transactional data usually desired by government agencies are never released to private parties, and breaches of this customary secrecy are rare. This confidential relationship is supported by more than custom: Banks are under a legal obligation to maintain the secrecy of their depositor's transactions. Although the duty of secrecy is not unqualified, the courts have made it clear that the banker functions as an agent in handling account information. He can release data only if consistent with that role.[96]

In their study of American data banks, Westin and Baker found that banks were generally sensitive about the information they maintained on customers:

> Protection of customer information from unauthorized or improper disclosure is also a critical aspect of maintaining good customer relations and has been reflected historically in a tradition of confidentiality applying to the banking transactions of individuals, companies, and organizations. Unlike

> Switzerland, however, where laws require secrecy in account and transaction information and make disclosures without consent of the customer or legal direction a criminal offense, American legislation has not spelled out such guarantees of confidentiality. Furthermore, American rules for business regulation, tax investigation, and law enforcement have often worked to open financial transactions between individual customers and banking enterprises to scrutiny by executive, legislative, and judicial agencies.[97]

These American statements generally reflect the Canadian situation as well. A brief from the Royal Bank of Canada to the Task Force on Privacy and Computers asserted that "any information provided by the customer to a bank is considered as 'privileged' between bank and customer. [It] is considered as the 'property' of the customer."[98] A federal official reported that Canadian banks fear consumer reprisals if they allow data about their customers to become known.[99] In a 1972 study of electronic banking systems, Gellman, who is a Canadian computer expert, concluded that "the banking industry in Canada has earned a well-deserved reputation for processing data accurately and for preserving confidentiality. This assurance of confidentiality is an important basis for success by the chartered banks. It could, therefore, be argued that the banking industry will probably continue to protect personal privacy in future, despite the new problems posed by increased automation."[100] The ability of financial institutions to control this situation may have lessened with increasing mechanization of procedures.

The policies of the Bank of Montreal can be regarded as typical of Canadian chartered banks. Its policies on confidentiality emerge particularly in connection with the dissemination of credit information. The bank considers its relationships with customers a confidential one, and the obligation of secrecy applies to all transactions in an account.[101] The conditions of employment form signed by new Bank of Montreal

employees reminds them of the importance of maintaining the secrecy of customer accounts; this is standard practice in the banking industry. The employee agrees at all times, even after ceasing to be employed by the bank, to maintain secrecy with regard to the bank's business and the business of its customers. The new employee also has to sign an agreement concerning conflict of interest, which includes the statement that "all employees are reminded that any bank is under obligation not to disclose to third parties the business of any customer, except where required to do so by law. This is a vital requirement of our business and is dealt with in detail in By-Law No. 13 of the Bank and in Topic 35-715-7 entitled "Credit Information."[102] Yet it seems surprising in light of the above that a booklet of "Welcome" presented to new Bank of Montreal staff, and entending to eleven pages in length, has no direct mention of confidentiality except again in connection with conflict of interest. The latter statement begins with the assertion that "banking, more than any other business, is founded on trust and confidence."[103]

Canada Trust, a leading trust company, has a new corporate policy on consumerism, which states explicitly that the customer "has the right to expect personal information to be treated confidentially within the company and within the law." The same policy also provides that the consumer "has the right to withhold any personal information not relevant to the transaction at hand, or not necessary within the law." Canada Trust also requires a strong "secrecy pledge" from all new employees:

> At the inception of my employment with Canada Trustco Mortgage Company and The Canada Trust Company, it was explained to me that one of the reasons our organization enjoys such a fine reputation is that all employees recognize the confidential nature of our business and co-operate in maintaining high ethical standards.
>
> Consequently, I pledge myself to observe the strictest secrecy on the subject of the affairs and

> the accounts of all customers and shareholders whether individual or corporate regarding which I may acquire information in the course of my duties including all matters pertaining to the administration of estates, trusts, and agencies of The Canada Trust Company.
>
> It is understood that this pledge will remain equally binding in the event of my termination for any reason whatsoever.

This pledge is incorporated in the single-page document used to set up new employees. Finally, a Vice-President of Canada Trust, who regularly reviews a file of letters of complaint written to the President, cannot recall a single complaint in recent years concerning breach of confidentiality of data.

Financial institutions will obviously have to confront a new level of challenge to the confidentiality of data as various forms of EFT are implemented. Although the Canadian Bankers Association does not foresee the advent of a "cashless society," it does anticipate the implementation of EFT: "It is fundamental to the banks' consideration of EFT systems that the traditional standards or privacy of customers' accounts will be maintained."[104] The use of the word "traditional" in this statement may be somewhat ambiguous. The CBA is also aware that "there has been some public concern that the new method of moving funds would adversely affect the customer's traditional rights of full control over the disbursement of his or her deposits and the privacy of records. Such concerns are groundless."[105] It will be clear from other sections of this Working Paper that such a degree of optimism seems exaggerated.

Nevertheless, it seems safe in Canada, if not always in the United States, for a customer to approach a relationship with a financial institution with an expectation of confidentiality. Justice Douglas expressed popular expectations in a 1974 dissenting opinion: "One's bank accounts are within the "expectations of privacy" category. For they mirror not only one's finances

but his interest, his debts, his way of life, and his civil commitments.... A checking account .... may well record a citizen's activities, opinion, and beliefs as fully as transcripts of his telephone conversations."[106] In an accompanying dissent, Justice Marshall also analyzed a customer's expectations: "The fact that one has disclosed private papers to the bank, for limited purpose, within the context of a confidential customer-bank relationship, does not mean that one has waived all right to the privacy of the papers... The customer of a bank, having written or deposited a check has a reasonable expectation that his check will be examined for bank purposes only - to credit, debit, or balance his account - and not recorded and kept on file for several years by Government decree so that it can be available for Government scrutiny."[107]

III.b. Disclosures by Financial Institutions

The literature on disclosures by financial institutions in the United States is quite revealing. Since 1972 the American Civil Liberties Union (ACLU) has been attempting to persuade banks to maintain strict standards for the confidentiality of customer information against any third-party demands for access. According to the ACLU, "people generally trust, when they write checks or deposit money in a bank account, that such transactions are confidential. Trust lies at the heart of the relationship between bank and customer. But the myth of the banker as the discreet, close-mouthed repository of financial confidences is just that - a myth. Individuals bank records are in fact accessible to the government for many purposes, both by statute and by long-established practice."[108]

ACLU standards for access to financial information include the requirement of a subpoena, notice of the subpoena to a customer, and time for the latter to challenge the subpoena before the data are divulged. Although the ACLU has received strong support from

some banks, it soon became clear, however, that even with the best of wills, banks could not protect their customers' privacy all by themselves." In comparison to private third parties, agents of the government are particularly compelling in seeking access to financial information, and banks like to maintain good relations with law enforcers. Thus the ACLU has had to turn from direct action with the banks to the courts and legislatures in order to assure the confidentiality of financial data. As the ACLU contended in a case consolidated with California Bankers Association v. Shultz, the "day-to-day practice of permitting "informal" access to bank records is, unfortunately widespread."[109] The government in return maintains that the banks own the financial records of customers, so that government access to such records has no impact on privacy. The ACLU and other privacy advocates argue that financial information belongs to the particular customer. Thus even before the implementation of EFT, the confidentiality of bank records is a problem in the United States.

In the United States, access by private third parties to financial information appears to be well-controlled. The exceptions to the rule of confidentiality include situations in which a customer consents to the release of information, where the bank's own business interests require disclosure, such as to collect an amount owed from an overdraft, and a situation where there is a public duty to disclose information, such as to prevent a fraud or crime.[110] The reported legal cases on confidentiality of financial information, which will be discussed further below, also support the view that access by private third parties is not a major problem: "In the very rare instances in this country in which a bank has released confidential information to a nongovernmental third party without the customer's consent, it has been held liable, although there has been no uniform theory on which liability has been based."[111]

The sheer volume of financial transaction information cannot help but contribute to confidentiality. There are more than 200

million bank accounts in the United States and more than 25 billion cheques written each year.[112] Yet it is also apparent that the mechanization of bank accounts and chequing services will facilitate access to such a large volume of data.

Under the Bank Secrecy Act of 1970, American banks are required to maintain microfilmed records of almost all cheques for one hundred dollars ($100.) or more. Because of the difficulty of sorting out the specific value of particular cheques, most banks in fact microfilm and retain copies of all cheques.[113] The same practice is standard in Canada. Thus even without EFT, banks already engage in the most extensive forms of record-keeping practices.

Formal and informal government access to financial transaction information is the most significant problem for confidentiality in the United States, and perhaps in Canada as well. When seeking formal access to financial information, the United States government has recourse to grand jury subpoenas, administrative summons, or search warrants.[114] In the recent case of U.S. v. Miller, the Supreme Court determined that an individual has no right of notification before the bank grants access to government agents. The various efforts that are underway to overturn this decision will be discussed further below. However, even if a customer learns about a pending government subpoena for his banking records, it is very expensive and time consuming to fight such a subpoena, either in Canada or the United States. American banks estimate that it costs them between $225 and $350 per request to contest a subpoena. There are also limited grounds on which a private individual can contest a government subpoena.[115] Even when the government does choose to obtain access to individual financial records by means of formal legal process, prevailing practices seem to grant very generous terms to the government agents. In U.S. v. Miller, both Georgia banks allowed government agents to search the accumulated microfilm records themselves, thus enabling the agents to view the cheques of other customers.[116]

Yet the most significant problem is the pattern of informal access by government agents to existing financial records: "The most serious threats to civil liberties are likely to occur when records are sought extrajudicially without issuance of notice to the affected individual."[117] EFT will further facilitate the existing information buddy system of unauthorized sharing of data. American commentators suggest that government investigators and law enforcers are able to exercise considerable pressure on bank officials and personnel, which often outweighs the official policy of refusing informal access. There has been considerable testimony in support of this view in Congressional Hearings during the 1970s.[118] Government agents are in a position to intimidate bank officers or employees, who are normally not lawyers and may be unaware of the legal requirements to test the validity of a request for access. These agents are in a position to become friendly with local bankers and to raise charges of disloyalty to the nation if the custodians of data become uncooperative. Informal access also saves both time and money for banks in comparison to the task of contesting a request for access. The existence of such patterns in the United States does not bode well for the future of disclosure under EFT.

The disclosure patterns of Canadian financial institutions with respect to other organizations, private third parties, and governments appear to be better regulated than those in the United States. The legal situation, which will be discussed in detail below, is in fact very clear.[119] The situation is typified by the policy of the Bank of Montreal to preserve secrecy as to the state of or matters concerning customers' accounts and their affairs, except where there is a duty of disclosure "under compulsion of law," a duty to the public to disclose, where the interests of the bank required disclosure, or where there is express or implied consent by the customer.[120] Although such a simple series of statements conform to the common law of banking, they could provide loopholes for financial

institutions to release customer information.[121] Canada Trust's policy on disclosure is to be very protective and concerned about the confidentiality of customer information. The strict policy is that there is no access to customer data in the branches without a court order. Access by government agents, such as the RCMP, takes place under a court order based on the Income Tax Act.

Discussions of the disclosure policies of Canadian financial institutions often fail to make a basic distinction between depository and credit information. Before the Privacy Protection Study Commission, "depository institutions (e.g. commercial banks, savings and loan associations, and credit unions) testified that they distinguish between their credit and their depository relationships when disclosing information to credit bureaus and other credit grantors."[122] The American institutions freely gave information about credit customers to the credit-grantor community, but would not disseminate the amount of, or existence of, a savings account to credit bureaus or other lenders. In practice, Canadian financial institutions also exchange information on credit ratings, especially bad risks.[123] In an earlier study of credit reporting practices, Professor John Sharp drew the following conclusion: "It appears, from widespread enquiries purused by the author, that banks usually - though not invariably - refuse to give information about deposits, but commonly pass on loan information."[124] The problem is that such a distinction is not established in Tournier, the legal case governing the confidentiality of Canadian banking records.[125] The prevailing situation for credit information is probably summarized in the Bank of Montreal form for personal loan applications, which reads in part as follows:

> The undersigned hereby authorizes the Bank of Montreal (the "Bank") to obtain any information required related to this application from any sources to which the Bank may apply and each such source is hereby authorized to provide the Bank with such information.

> The Bank is furthermore hereby authorized to disclose, in response to direct inquiries from any other lender or any credit bureau, such information concerning the loan account of the undersigned as the Bank considers appropriate, and the undersigned agrees to indemnify the Bank against and save it harmless from any and all claims in damages or otherwise arising from any such disclosure made by the Bank.[126]

This type of expansive contracting out on the part of financial institutions should be severely limited in the interests of privacy and confidentiality.

There are also questions about the extent to which the implementation of policies on confidentiality are in fact monitored by financial institutions. There are suggestions that employees of chartered banks hear little about the importance of confidentiality during training programs, and that practices with respect to confidentiality vary from branch to branch. There are regular conflicts in branches of financial institutions between protecting confidentiality and furnishing service to customers, such as in responding to telephone inquiries about the financial status of a person's account. It is inevitable that the press of business does not always permit the verification of the identity of a customer. Law enforcers are generally required to show a good reason for obtaining access to financial information and some form of legal authority. There are also suggestions that it is difficult to impress young bank personnel with the importance of confidentiality. The application form used for the Bank of Montreal ATM card also contains a broad waiver for releasing information, which is typical of the heavy burden placed upon customers. An applicant is required to sign a release form consenting "to the disclosure of any information concerning the undersigned to any person with whom the undersigned has or may have financial relations..." Such a blanket release is too generous for any type of EFT application.

III.c. Security

Although in recent years considerable attention has been

paid to maintaining the security of computers against criminal acts, it is generally agreed that computer systems are vulnerable to unauthorized access and that absolute protection of security is impossible.[127] Data thefts can easily remain unnoticed. It has been suggested that the limited attention sometimes paid to the problems of computer security is partly because security safeguards are optional items on software and hardware. The simple technical feat of breaching the security of a particular computer system is not a major undertaking, unless adequate safeguards exist.[128]

For the obvious reason that they handle large amounts of money, financial institutions have had a substantial concern for security for a long time. In the early 1970s, Westin and Baker found that the "Bank of America proved to have the most expensive and costly security measures for its computerized and manual records of any private organization that we visited."[129] Banks are particularly threatened with significant financial losses if security is breached or services are disrupted. Yet it is also evident that the advent of mechanized banking substantially increases the risk of breaches of security in computer systems. There are at least four locations for unauthorized access in EFT: the use of a stolen access key card and PIN at a remote terminal, access by employees located at remote access terminals, access by employees or outsiders at the central processing unit, and wire-tapping of communications lines.[130] The major IBM study on data security concluded that "it is possible, of course, to gain access by technologically sophisticated methods to data stored in the system. But information can usually be obtained in much less complicated ways."[131] In 1972 officials at the Bank of America in California viewed "embezzlement of money rather than leakage of personal information as the primary threat from persons getting unauthorized access to data."[132]

Although NCEFT regarded a full-scale system of EFT as generating a new level of risk, it viewed the problem of data security as one of extending current banking applications. The

Commission concluded that the limited experience to date with criminal penetration of EFT systems "shows that actual loss from fraud is low."[133] In early 1977, a survey of 1260 American banks using EFT systems found one-third reporting small losses averaging less than $100 per occurrence because of security problems with EFT. Evidently the problems were not difficult to correct.[134] Examples of much larger losses are also known.

The Privacy Protection Study Commission thought that previous experience in processing bank credit cards would be useful in connection with the protection of privacy, confidentiality, and security in EFT.[135] The Chargex or Canadian Bankcard System has considerable concern with data security. At the National Security Conference of Canadian Financial Institutions in Toronto on November 15, 1977, J.D. Hamilton, of the Chargex organization, who is also president of the Canadian Bankcard System, discussed "Security in the Credit Card Field." Since Chargex makes heavy use of in-house data-entry terminals, it limits the number of cathode tubes in an entry unit and thus restricts access by tellers to the entire data system. Chargex and Master Charge program restrictive words (passwords) to control access. They also limit the types of functions that can be performed at a particular terminal. All data entries made from a Chargex data-entry unit are uniquely identified with a terminal, which is standard practice in financial institutions generally. There is also a program in use to identify abnormal entries. The existing system also limits the number of authorizations on a particular account in a particular period. Hamilton correctly regarded audit trails as a crucial practice, because this makes it possible to trace all data entries back to a particular source. Audit trails discourage dishonest data entry. Such experience with data security in the bank credit card field can be and is readily applied to computerized banking.

Since procedures currently used in connection with on-line banking in Canada are the thin edge of the wedge for a full-scale

EFT system, existing practices merit attention. A recent survey of attitudes toward privacy among data processing managers of large organizations in Toronto revealed that banks and telecommunication companies "consider data security and privacy as an integral part of doing business."[136] The Bank of Montreal has all of its branches on-line to the central data processing centre in Toronto. Information is currently transmitted over Bell Canada telephone wires without scrambling or encryption of the data. Normally only the account number and a limited number of digits from the name of a particular customer are transmitted in connection with a particular transaction, so that interception of personal data would not be very revealing. Tellers who use the terminals only have access to their branch customer files for browsing or transactions. Each teller has a password controlling his or her access to a terminal. These passwords are changed at least once a year, or if a person resigns or has his or her password exposed to another individual. The Bank of Montreal system furnishes supervisors with the capacity for complete surveillance over users of terminals, because all data keyed into a terminal are recorded in a printed form in a journal roll for auditing purposes. A simple search for and retrieval of personal data, such as account balances or a home address, is documented. However, the Bank also produces regular print-outs of account activity, which are available in the local branches. Hence a teller seeking unauthorized access to data about a local customer now simply has a choice of a computerized or a manual search.

Canada Trust appears to have an admirable series of security procedures and practices. Access to the central processing unit in London is carefully controlled. The access by tellers in the branches to the savings data base is monitored by a transaction register. Each terminal produces a complete record on paper or electronic tape of every activity by a teller on the terminal; these transaction registers are reviewed by management on a regular basis. Tellers thus function under the watchful eye of

"Big Brother." There is no after hours access to the central data base from branches, which are closed off at a certain time. The duties and responsibilities of the data processing staff are divided among product managers, systems analysts, and programmers. Changes in programs made by the latter are monitored. Personnel are encouraged to leave clean desks at night and to lock up files of print-outs. Canada Trust has tested the security of its telephone lines against wiretapping of electronic impulses; its concern to protect against fraud has a simultaneous benefit for the confidentiality of data. The company believes that it is quite difficult to identify an appropriate telephone line and to use information acquired in electronic form for fraudulent purposes. Finally, Canada Trust has added a variety of security features to its new COFIS information system to protect the interests of the company and the customer. To date, COFIS uses passwords but not encryption.

Although inspired less by concern for the confidentiality of customer than data, the challenge of computer fraud, financial institutions in Canada have thus bought and developed significant data security technology.[137] More sophisticated methods of protection, such as encryption of data, are used by the Toronto-Dominion Bank in particular. It is also common to change access control keys at frequent but unspecified intervals. An insider reported to a journalist that the "access defense system" used by the Bank of Montreal is almost unbreakable, because it has sacrificed access speed to have as secure a system as possible.

Concern for security of computer operations is obviously widespread among Canadian financial institutions. An assistant general manager of the Banque Canadienne National (BCN) reports as an example of concern for security that "at head office, our systems development people are entirely separate from our operations people, and no program changes can be made without proper authorization."[138] This is a standard practice. The

Vancouver City Savings Credit Union uses an on-line banking system developed by Geac Canada Ltd. Its security features include individual password structure, physical protection from unauthorized communications access, and a signature verification and display system. The latter involves displaying both account information and the signature of a customer on the same screen for a teller.[139] In the IBM 3600 Finance Communication System, the controller, which is a mini-computer, can be programmed to determine what levels of information each operator is allowed to access, so that security and privacy can be protected.

Since automated tellers and cash dispensing machines are in fairly common use in North America, a fair amount is known about their experience with physical security. The experience of a data processing firm in Florida, which handles data processing in thirty-one banks, illustrates a basic problem. The firm services ATMs in eight locations on the basis of customer information files. The firm learned that their minimum-wage employees were accessing these files at night, transferring a quarterly savings account to their own customer information file numbers, and then returning the funds after a weekend was over with a profit of perhaps $10,000. An audit trail existed for such transactions, but it was voluminous and difficult to follow. These employees obviously had access to a full range of personal data. The firm's partial solution was to initiate operator sign-on codes, authorization files, and various restrictions on access by personnel.[140]

The IBM 3614 (and the new 3624) Consumer Transaction Facility or ATM have a variety of protections for privacy and confidentiality built into the system. When the 3614 is operated in an on-line mode, every customer record can be kept up to date and accessed in the central system. The system itself can note attempts at unauthorized usage, such as multiple attempts at entering a personal identification number. The functional area of the machine

has a recessed keyboard to provide privacy and confidentiality.[141] IBM has designed protections to prevent the wiretapping of the ATM in such a manner as to activate the cash dispenser. In particular the system makes use of "an elaborate method of scrambling messages on a line by using a frequently changed numerical key, to make the data useless to anyone tapping the line." The ATM encrypts the sensitive elements of every message, which are decrypted at the host computer. The encryption algorithms available are either the U.S. Federal Information Processing Data Encryption Standard or the IBM 3614 Alternate Encryption Technique. PIN's are "double encrypted," so that they never appear "in the clear" anywhere in the system. Every cash transaction is also rendered unique by means of a non-resettable control counter.

Although laymen (such as this writer) tend to be impressed with the current capacity for security, the experts continue to emphasize the limitations of existing protective systems. Earl Ward, a specialist in banking automation, informed the National Commission on Electronic Fund Transfers of the security weaknesses in existing ATMs, including the PIN, the use of cards, and the process of encrypting. He even included suggestions about how ATM systems could be beaten.[142] The New York Times recently reported on the extent of electronic fraud accompanying the move toward tellerless banking and how the banks are responding to the challenge.[143] A study by the U.S. Government Accounting Office has revealed that the security program of the Internal Revenue Service does not adequately protect the confidentiality of tax data and provides widespread opportunities for unauthorized disclosures.[144] Thus it is clear that the battle to protect confidentiality of personal data in EFT and computerized banking will be a continuous one.

The variety of security devices available to protect ATMs also illustrates the potential challenge of security measures to personal privacy. Frisco Bay Industries of Canada Ltd. sells

the "Frisco Bay Anti-Fraud Protection for Automatic Teller Systems." The device in question is an automatic teller surveillance system based on a camera that operates twenty-four hours a day. During any transaction at the ATM the camera is activated to take two pictures, one at the insertion and the other at the withdrawal of the card; "each film frame shows the exact time and date of the transaction as well as the customer." Control over the disposition of such film poses some interesting problems for privacy.

Seven Canadian chartered banks are members of S.W.I.F.T., the Society for Worldwide Inter-Bank Financial Telecommunication. The measures in force in SWIFT for protecting data security are an illustration of the capacity of current banking practices to protect confidentiality, although some security specialists even question the adequacy of SWIFT practices. The system links together 500 international banks in 17 countries in order to transfer messages between banks. The starting date of the system for Canadian and American banks was September 26, 1977.[145] The Bank of Montreal asserts that SWIFT is "the first step toward international electronic banking of the future; the system allows members to exchange, safely and rapidly, private and confidential messages, to transfer funds and to confirm financial information."[146] All banks in a particular country are connected to a single computer system known as a concentrator, which for Canada is located in Montreal. The concentrators are in turn controlled by two central computers, known as switches, in Holland and Belgium. The banks are responsible for security between the particular bank and the concentrator, while SWIFT worries about transmissions between concentrators through the central switches. It is reported that "some banks have chosen to encrypt or scramble between their terminal and the concentrator and others have not been able to cost justify this added precaution."[147] The Bank of Nova Scotia is in the former category.

SWIFT has provided extraordinarily detailed and complex provisions for the security of its system. The elements include

identification and authorization for use of the system, prevention of transmission errors, assurances of transmission privacy and physical security, and provisions for personal reliability, software control, and central file protection. A log-in code enables a bank to initiate identification for the SWIFT system. The user changes at each attempt and is sequenced: "Each message sent must contain an input sequence number which if incorrect will force the user to log in with the next code." There is also an output sequence number for each message delivered by the system, which is checked automatically by the user terminal. From the perspective of transmission privacy, all data on international lines are scrambled to assure confidentiality through the use of what is known as the authenticator. The process begins with a system similar to the one used to test the authenticity of messages between banks. Keys are exchanged for codes. In the SWIFT system, all of the particular message is used in the calculation, and the algorithm for mathematical processing is infinitely more exomplex than with the inter-bank system. The encryption cannot be computed manually. Any change in any character in the message will produce a failed test at the other end.[148]

III.d. The Current Legal Situation

At first glance the legal situation with respect to the confidentiality of bank records is clear cut. The rare common law cases on the point date back to England in the middle of the nineteenth century. One recent observer has concluded that "banks voluntarily act in confidence and pride themselves on this high ethical standard. The banks' strict adherence to secrecy is the reason that there have been only ten cases on the issue of disclosure in Anglo-American jurisprudence."[149] The mainstream of cases requires that in general banks will not disclose information about customers to a third party because of an implied contract between the banker and his customer.

> It is an implied term of the contract between a bank and its customer that the bank will not disclose to

> third persons, without the consent of the customer expressed or implied, either the state of the customer's account, or any of his transactions with the bank, or any information relating to the customer acquired through the keeping of his account, unless the bank is compelled to do so by order of a court, or the circumstances give rise to a public duty of disclosure, or the protection of the bank's own interests requires it.[150]

This statement of the law in Canada by Falconbridge derives from the headnote of Tournier v. National Provincial and Union Bank of England in 1924.[151] The case involved a bank manager held liable for disclosing to a third party that one of his customers had written a cheque to a bookmaker. Tournier is frequently cited as establishing a bank's implied contractual duty of secrecy.[152] It settled Canadian law on this point.[153] The case was cited with approval in the recent Ontario case of Haughton v. Haughton, which involved an attempt to have a bank manager testify about the financial affairs of a husband in a proceeding for alimony. Counsel for the bank manager objected to his answering any questions or producing any bank records relating to the affairs of a customer without the approval of the customer or without a court order. Since the customer would not consent in this case, the court determined that "counsel for the witness was right in arguing that a Court Order is necessary before the witness can answer the questions asked by the plaintiff herein."[154]

In its treatment of the topic of banking, the Canadian Encyclopedic Digest discusses the question of confidential relationships: "A duty rests on a bank not to make any disclosure of the particulars of a customer's account without his express or implied instructions to make such disclosure... A bank manager is precluded from producing any bank records relating to the affairs of a customer without the customer's approval or without a court order..."[155] Although the Canadian cases seem clear on the requirement of confidentiality, it will readily be seen how far the specifics of the various cases diverge from EFT types of problems.

In reviewing the firm adoption by Canadian courts of the doctrine of confidentiality with respect to the details of customers' deposits, current accounts, and personal checking accounts, Professor John Sharp noted that "there is little doubt that the bank which makes disclosures in this area, unless it falls within one of the exceptions, will be liable to its client."[156] These common-law exceptions were established in the Tournier decision. The legal duty of a bank - arising out of contract is thus a qualified and not an absolute duty at common law.[157] The four exceptions to the rule of confidentiality are disclosure under compulsion of law, where there is a duty to the public to disclose, where the interests of the bank require disclosure, and where the disclosure is made with the express or implied consent of the customer. Lord Diplock explained the first exception in a recent case: "For example, in the case of banker and customer, the duty of confidence is subject to the overriding duty of the banker at common law to disclose and answer questions as to his customer's affairs when he is asked to give evidence on them in the witness box in a court of law."[158] The third exception would be best illustrated by a prosecution against a customer by a bank for fraudulent transactions. Disclosure with the consent of the customer is a self-explanatory case, but the second exception is much more difficult. There does not seem to have been a litigated case where a bank disclosed information because of an alleged duty to the public. It has been suggested that evidence of a customer's dealing with the enemy in wartime might be an example.[159]

There are some federal and Ontario statutory controls on the disclosure of financial information, which are relevant to the discussion of confidentiality. Although there are unfortunately no provisions on confidentiality of personal information in the federal Bank Act, or the Ontario Loan and Trust Companies Act, there is a strong provision in the Ontario Credit Unions and Caisses Populaires Act: "Except as provided in this Act, no member or other person has the right to inspect

the books of a credit union."[160] In addition, "no person, unless he is an officer of the credit union or is specifically authorized by a resolution thereof, has the right to inspect the loan or deposit account of any other member without such other member's written consent."[161] These provisions may make credit unions the best protected Ontario financial institutions. They might even resist access by the RCMP, since there is no provision for access by means of a court order, only by authorization of the credit union.

The Canada Evidence Act also regulates disclosure of financial information:

> A financial institution or officer of a financial institution is not in any legal proceedings to which the financial institutions is not a party compellable to produce any book or record, the contents of which can be proved under this section, or to appear as a witness to prove the matters, transactions and accounts therein recorded unless by order of the court made for special cause.[162]

The necessity for a court order establishes the basic law on disclosure. There has been no reported litigation under this section, which is permissive and not mandatory. The Evidence Act also provides that upon application of a party to a legal proceeding, a "court may order that such party be at liberty to inspect and take copies of any entries in the books or records of a financial institution for the purposes of the legal proceeding; and the person whose account is to be inspected shall be notified of the application at least two clear days before the hearing thereof...."[163] The requirements of relevance and due notice are strong protections. Thus subpoenas issued by attorneys to parties or financial institutions are reviewable in court.

The Ontario Evidence Act has provisions comparable to the federal statute on the same matters. It applies to banks under

the federal Bank Act and the Province of Ontario Savings Office:

> A bank or officer of a bank is not, in an action to which the bank is not a party, compellable to produce any book or record the contents of which can be proved under this section, or to appear as a witness to prove the matters, transactions and accounts therein recorded, unless by order of the court of a judge made for special cause.[164]

A second provision requiring a court order for the production of books is identical to the provision of the Canada Evidence Act, cited above except that the applicability is to banks and not financial institutions in general.[165]

The Ontario Consumer Reporting Act of 1973 has some valuable protections for the confidentiality of consumer data, which will only be mentioned briefly here because it is doubtful that they apply to financial institutions generally. They would be applicable if banks could be defined as "consumer reporting" agencies under the terms of the Act. It provides that a consumer reporting agency can only furnish information from its files in response to a court order, the authorization of a customer, or for various credit-granting purposes.[166] It is illegal for a person to knowingly obtain information from such files for any other purpose.[167] The Act limits the information that may be collected by a consumer reporting agency, which should be applied to the credit activities of all financial institutions.[168] Finally the Act provides that "no person extending credit to a consumer shall divulge to other credit grantors or to a consumer reporting agency any personal information respecting the consumer except with the consent of the consumer or on his referral unless he notifies the consumer in writing at the time of the application for credit that he intends to do so."[169]

The mainstream of the few American cases on the question of banking confidentiality also rests on the doctrine of implied

contract. Until recently, the leading American case concerning the confidentiality of customer information was Peterson v. Idaho determined in the Supreme Court of Idaho on December 8, 1961.[170] The plaintiff sued the bank for invasion of privacy, when the bank disclosed information about his personal bank account to his employer. The Idaho court rejected the plaintiff's claim on the grounds of invasion of privacy, but accepted this claim on the basis of the implied contract between the customer and the bank "that no information may be disclosed by the bank," unless authorized by law and the customer: "It is inconceivable that a bank would at any time consider itself at liberty to disclose the intimate details of its depositors' accounts. Inviolate secrecy is one of the inherent and fundamental precepts of the relationship of the bank and its customers or depositors."[171]

The doctrine of implied contract also prevailed in a 1969 Florida case.[172] Before this decision, Florida banks were bound to the secrecy of customer information only by their ethical practices. This particular case changed the prevailing morality into law: "The principal case adds Florida to the small list of states that hold a bank owes a legal duty of secrecy to its customers."[173] In Milohnich, the First National Bank of Miami Springs was accused with unlawfully releasing information about its depositors to third parties. The Florida Third District Court of Appeal, quoting approvingly from the Peterson v. Idaho and Tournier v. National Bank decisions, concluded from such leading cases that "a qualified duty of non-disclosure appears to be evolving in both England and America."[174]

A series of federal statutes and Supreme Court decisions since 1970 have made the protection of the confidentiality of financial information more difficult in the United States. The problem essentially began with the enactment of the Bank Secrecy Act of 1970, which required banks to keep records on the financial transactions of customers for an extended period of time.[175] The

premise of this mis-named statute was that "an effective fight on crime depends in large measure on the maintenance of adequate and appropriate records by financial institutions."[176] One of the pertinent implications of the Bank Secrecy Act for Canadians is that similar considerations favoring law enforcement, but at the same time threatening personal privacy, may at some point become relevant in Canada as well. The Bank Secrecy Act has been much criticized by privacy experts and by the financial institutions themselves on the grounds of concern for privacy and confidentiality.[177]

The constitutionality of several specific provisions of the Bank Secrecy Act was upheld in California Bankers Association v. Shultz.[178] The majority determined that the statute was really designed to control crime through the policing of secret foreign bank accounts. The court upheld the portions of the statute which mandated specific forms of bank record-keeping, but ruled that it was premature to rule on third party aspects of the statute. The statute is not unconstitutional, especially so long as access to bank records is controlled by the existing "legal process."[179] The Bank Secrecy Act ultimately illustrates how far a government can go in requiring bank record-keeping for law enforcement purposes, a process which EFT will only make easier.

The Supreme Court did display some sensitivity to financial privacy in California Bankers Association. In a concurring opinion Justice Powell, joined by Justice Blackmun, asserted that a significant extension of the regulations on reporting requirements under the Bank Secrecy Act would pose substantial and difficult constitutional questions: "Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy."[180] In a

dissenting opinion Justice Douglas, who was joined on these points by Justice Brennan, asserted that the Bank Secrecy Act requires banks to spy on their customers: "Customers have a constitutionally justifiable expectation of privacy in the documentary details of the documentary details of the financial transactions reflected in their bank accounts. That wall is not impregnable. Our Constitution provides the procedures whereby the confidentiality of one's financial affairs may be disclosed."[181]

The NCEFT concluded that the Bank Secrecy Act, California Bankers Association, and the more recent case of United States v. Miller were all important for EFT, "because it is likely that EFT transactions will fall within their purview."[182] The Miller decision dealt the most devasting blow to the prevailing theory that a customer had some rights to the confidentiality of his banking information. One commentator has suggested that the Miller decision makes the value of the cases previously discussed here on bank confidentiality "somewhat dubious."[183] It involved a Georgia moonshiner, whose financial records were acquired from two banks under government subpoena. The records were maintained under the Bank Secrecy Act. The two banks did not notify the respondent Miller of the government subpoena. The Fifth Circuit held for Miller, but the Supreme Court reversed the decision by majority vote. It determined that the defendant Miller had no right or interest in protecting his financial records from subpoena, nor any legitimate expectation of privacy for his cheques and deposit slips:

> The cheques are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act....[184]

The majority decision written by Justice Powell further concluded that "the depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government."[185] The court further determined that the records of the customer were in fact "the business records of the banks."[186] In a strong dissenting opinion in the Miller case, Justice Brennan quoted extensively from the "excellent opinion for a unanimous court" in Burrows v. Superior Court, which will be discussed further below.[187]

Both the Bank Secrecy Act and the Miller decision have been subjected to strong criticism. One commentator suggested that in the Miller decision "the Supreme Court now appears to have an unarticulated rule under which the government has an absolute right to know the contents of an individual's bank records."[188] The commentator concluded that after Miller, "an individual who wants to maintain the privacy of his financial affairs must deal entirely in cash because otherwise he abandons his fourth amendment right by divulging these affairs to third persons."[189] On the basis of the Bank Secrecy Act, a number of representatives of the banking industry have been urging Congress to enact legislation to protect the privacy of customers' records.[190] Robert E. Smith, a lawyer and publisher of the Privacy Journal, concluded in a public discussion on April 10, 1976 that "the current case law and statutory law protecting bank confidentiality is extremely inadequate."[191] Others agree that American common law, statutes, and constitutional law are inadequate to deal with the problems for privacy and confidentiality posed by EFT.[192] Some of the federal legislation for credit protection has been suggested as analogous models for EFT legislation.[193] The only Congressional response actually enacted to date is the provision in the Tax Reform Act of 1976 giving a bank customer the right to challenge access by the Internal Revenue Service to his bank records on the basis of an administrative summons. This remedies for IRS only the lack of standing of an individual to contest

government access under the Miller decision. This situation is now controlled by a valid legal process.[194]

At least thirty-two American states have enacted legislation governing EFT, but most enactments pay almost no attention to such consumer interests as privacy, security, and liability.[195] There are no comparable Canadian laws. State EFT legislation primarily deals with such issues as branch banking and the sharing of EFT facilities, which suggests that the acts owe more to industry initiative than to the concerns of the public.[196] At least four state statutes simply mention the importance of maintaining physical security in an EFT system.[197] The Kansas enactment for Savings and Loan Associations includes a specific requirement for security features, including "provisions that will not allow the data communications linkage to be vulnerable to a wire tap or intervention from a foreign source."[198]

EFT enactments by Iowa, Oregon and Florida in 1975 included some consideration of privacy issues.[199] The Iowa EFT law attempts to ensure that only banks have access to customer information essential for a transaction.[200] The Oregon enactment determines that an EFT system should not be used to obtain information about a customer's account without the customer's approval.[201]

The Florida EFT law has the most comprehensive procedures to protect the interests of consumers. Security safeguards are required: "Every owner of a remote financial service unit and every bank using a remote financial service unit shall adopt and maintain safeguards to insure the safety of funds, items, and other information, which safeguards shall include security devices consistent with the minimum requirements specified under the Federal Bank Protection Act or such alternative security precautions as are approved by the department."[202] Customers have a right to certain information: "The department shall have

the authority by rule to require each bank operating pursuant to this section to supply information to customers using remote financial service units [concerning] the bank's consumer protection policies, including the rights and liabilities of consumers and protection against wrongful or accidental disclosure of confidential information."[203]

The Florida EFT act requires banks to file annual reports with the legislature, which shall "discuss the procedures for the protection of a customer's privacy and confidentiality of account information and discuss who has access to a customer's account information and under what circumstances."[204] Banks can be held liable for failing to maintain reasonable procedures to minimize losses to its customers from unauthorized withdrawals.[205] Information acquired through EFT systems is governed by applicable law with respect to dissemination and disclosure.[206] Finally, the statute includes procedures and penalties for wrongful disclosure of information and procedures for complaints of unsafe and unsound banking practices involving remote units.[207]

California is the English-speaking jurisdiction that has made the most progressive efforts to cope with the issues of confidentiality of both banking and EFT records. There are no comparable Canadian developments. The California Supreme Court reached a unanimous opinion in Burrows v. Superior Court, which is directly at odds with the Miller decision of the United States Supreme Court.[208] Burrows was an attorney suspected of misappropriating a client's funds. A detective sought and received informal access to his financial statements at a bank. A trial court determined that the search and seizure of his bank records was reasonable, but the Supreme Court of California accepted the view that a bank customer had a legitimate expectation of privacy and that there was a consequent requirement of legal process for obtaining access to individual bank records. In California a depositor thus enjoys a right of privacy, even though the Burrows decision came before Article 1 of the California decision was amended by voter initiative of November 5,

1974 to make privacy an inalienable right.[209]

In the Burrows decision, the Supreme Court of California were of the opinion that:

> It cannot be gainsaid that the customer of a bank expects that the documents, such as checks, which he transmits to the bank in the course of his business operations, will remain private, and that such an expectation is reasonable... Representatives of several banks testified at the suppression hearing that information in their possession regarding a customer's account is deemed by them to be confidential.... A bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes. Thus, we hold petitioner had a reasonable expectation that the bank would maintain the confidentiality of those papers which originated with him in check form and of the bank statements into which a record of those same checks had been transformed pursuant to internal bank practice.[210]

The Supreme Court also determined that "for all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."

> In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography. While we are concerned in the present case only with bank statements, the logical extension of the contention that the bank's ownership of records permits free access to them by any policy officer extends far beyond such statements to checks, savings, bonds, loan applications, loan guarantees, and all papers which the customer has supplied to the bank to facilitate the conduct of his financial affairs upon the reasonable assumption that the information would remain confidential. To permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other

> traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, opens the door to a vast and unlimited range of very real abuses of police power.[211]

The California Supreme Court has further developed the doctrine of financial privacy since Burrows. In a 1975 decision a unanimous Supreme Court of California set standards under Burrows for civil discovery of bank records.[212] The court held that compelled discovery must be conditioned on balancing the right of discovery of relevant facts by civil litigants against the bank customers rights of reasonable privacy regarding their financial affairs. The court determined that before a bank produces a customer's confidential records it must take reasonable steps to locate the customer, inform him or her of the discovery proceedings, and allow the person reasonable opportunity to object and to seek appropriate protective orders.[213] In subsequent decisions the California high court has also created an exception to financial privacy in a situation where the bank is a victim of fraud and has a "legitimate interest in self-protection from wrong-doing."[214]

This Working Paper will ultimately argue that jurisdictions in Canada should follow the lead of the California Supreme Court rather than the United States Supreme Court when it comes to further determinations on the confidentiality of information in financial records. It is noteworthy that in a lecture at the Gonzaga University School of Law on April 20, 1977, Chief Judge David L. Bazelon of the U.S. Court of Appeals for the District of Columbia found the California Supreme Court, rather than the United States Supreme Court, "more sensitive to privacy, but also closer to reality" in ruling that bank customers have an expectation of privacy, and therefore a right to confidentiality, in their personal bank records.[215]

California has also set the pace for other North American jurisdictions by enacting the California Right to Financial

Privacy Act of September 28, 1976, which codifies the doctrines of Burrows and its progeny.[216] The California legislature found and declared that "the confidential relationships between financial institutions and their customers are built on trust and must be preserved and protected." The Financial Privacy Act is designed "to clarify and protect the confidential relationship between financial institutions and their customers and to balance the citizen's right of privacy with the governmental interest in obtaining information for specific purposes and by specific procedures as set forth in this chapter."[217] A "financial record" is defined as "any original or any copy of any record or document held by a financial institution pertaining to a customer of the financial institution."[218] Requests for access to financial records for the purposes of a civil or criminal investigation by a government official should be described with "particularity" and be consistent "with the scope and requirements of the investigation giving rise to such requests."[219] A financial institution is also required to maintain an audit trail for a period of five years of individuals obtaining access to customer financial records.[220] The statute contains detailed provisions of how a customer can authorize disclosure of personal information and how requests for access by administrative summons or subpoena should be handled.[221]

The California financial privacy act primarily controls access to financial data by government agencies. The states of Illinois and Maryland have since passed financial privacy acts establishing conditions under which banking records may be disclosed to anyone pursuant to compulsory legal process. The basic principles are that legal process must govern any release of personal data and that customers must receive specific notice of the pending request for access.[222]

IV SOLUTIONS AND REGULATORY MODELS

IV.a. Self Regulation

Canadian financial institutions, computer manufacturers, and computer service bureaus involved in the development of EFT systems should continue their efforts at self-regulation in the interests of privacy, confidentiality, and security. Since EFT is at an early stage of development, these organizations should be able to build adequate concern for these societal values into their various systems and avoid more government regulation. The goals of self-regulation in the interests of privacy, confidentiality, and security are fairly evident. Financial institutions in particular require basic, precise and enforceable rules for the collection, protection, and disclosure of personal information, which will balance the needs of the institution and the interests of the individual.

Consumers want a code of fair information practices to apply to their financial data. Part 4 of the Canadian Human Rights Act of 1977, which will be discussed further below, incorporates elements of fair information practices, such as the principle that information in federal data banks should only be used for the purpose for which it was originally collected. Alan F. Westin has developed a similar set of principles for the protection of health data, which can be applied in part to EFT.[223] Financial institutions should be expected to set appropriate limits on the collection and recording of personal and financial transaction information. Release forms whereby customers agree to the dissemination or circulation of personal information should be specific and limited in scope. Customers should have a contractual right of access to check the accuracy of stored data. Financial institutions should apply appropriate data security measures. The adequacy of existing protections should be monitored by independent audits and periodic management reviews.

Financial institutions could readily limit the descriptive

information about purchased items that are entered into EFT systems, but customers might at the same time have to sacrifice at least a part of their monthly descriptive billing statements in order to reduce the risk of invasion of privacy. It should not be necessary to record what was purchased, only the amount of the purchase and when and where it took place. Some type of information segregation should also be built into EFT. The information furnished by customers in opening accounts or seeking loans should be separated from financial transaction information. If personal information is entered into computerized form, then it should be separated into more controlled types of files than ordinary financial transaction information. Retail POS networks should normally not permit access to sensitive personal information, such as is included in credit applications. POS networks should probably not permit the use of a POS card to make extremely small purchases, such as a newspaper, which would limit the capacity of the system for surveillance.

Thus banks themselves should severely regulate and limit the kind and amount of personal information they enter on computers, especially in an on-line mode.[224] The use of EFT data for marketing purposes should be severely restricted; perhaps informed consent for such uses should be required from individuals. The availability of data in an EFT network for analytical or browsing purposes should be limited. It would appear to be undesirable to build a capacity into the system to search for various types of data pertaining to a particular person. The public has developed considerable misunderstandings concerning the current potential for surveillance in such computerized systems as airline reservations and major credit card systems.[225] If EFT programs are limited in terms of the capacity for searching and matching data, public anxieties could be severely reduced.

The formulation of standards by financial institutions for the protection of privacy and confidentiality is only the first step. These must also be publicized and enforced at the branch

level. Personnel of financial institutions will have to be indoctrinated on a regular basis concerning the importance of privacy and confidentiality. Financial institutions and their associations should engage in public relations to publicize their degree and mode of concern for privacy and confidentiality.

The same needs and practices discussed above should apply to computer manufacturers and service bureaus. Specific controls for the confidentiality and security of data should be and probably are included in contracts between financial institutions and service bureaus.[226] In the process of promulgating and enforcing desired standards for privacy and confidentiality, the computer industry should develop ethical codes of conduct and guidelines for employees, operators, programmers, tellers, and other key personnel. The Association For Computing Machinery, for example, has a Code of Professional Conduct.[227] An adequate ethical code should include some type of meaningful sanctions, which should also be publicized.

The Association of Data Processing Service Organizations (ADAPSO) in the United States has formulated a policy statement on privacy and security.[228] Its recommendations include periodic audits, the segregation of duties between programmers and operators, the bonding of key EDP personnel, the rotation of operators, the coding of confidential data, and the requirement of a secrecy agreement as a condition of employment. The Canadian Association of Data Processing Organizations has not adopted similar recommendations. The Canadian Standards Association has a committee on data security chaired by Professor John Carroll of the University of Western Ontario. Thus there are no current Canadian guidelines on computer security that governments and financial institutions can use as a model. The federal Treasury Board's Guide on EDP Administration (1972) is outdated. One promising development is a series of manuals forthcoming from the Systems Security Branch of the RCMP. It is also reported that a new organization of Canadian

EDP auditors will work on computer security problems through its Toronto chapter.[229]

The consumers' reactions to the issues of privacy, confidentiality, and security in EFT are so potentially explosive that the organizations discussed above would be well advised to voluntarily adopt protective measures. As the NCEFT concluded in its Interim Report, "consumers are more concerned about drawbacks of EFT than about potential benefits. The Commission believes that certain of the consumers' concerns about EFT are justified and that some potential advantages of the system will depend upon incorporating consumer protection features."[230] Since the trend today in the privacy field is for the enactment of data protection statutes, the same institutions would be well advised to avoid further government regulation, if possible. Although data protection legislation to date has primarily concerned data banks in the public sector, the next target is the private sector. This stage has already been reached in Sweden, West Germany, and France.

A final motivating factor toward self-regulation should be the potential liability of financial institutions and computer service bureaus for unauthorized disclosure of personal data. Although most of the court cases in the context of bank confidentiality arise out of criminal proceedings, an aggrieved customer might also have the option of suing the financial institution or other organization for breach of confidentiality.[231] In fact, consumers would be well advised to push for the imposition of liability on financial institutions as one form of self-regulation.

Financial institutions face conflicting pressures in the area of confidentiality and security. They have little incentive (except the force of habit) to collect or mechanize more information than they need for efficient operation, so that the cost factor

works in favor of privacy. On the other hand, computer manufacturers seem to leave to their customers the responsibility for "incorporating protective measures to safeguard the privacy of data."[232] IBM designs general purpose hardware with some common, automatic security built-in for operating procedures. But security items are primarily designed as separate features; the customers decide on their own needs in the context of tolerable costs in a competitive environment. Optional security features are fortunately becoming better and more cost effective. Most measures required for security in particular necessitate cost justification and the expenditure of significant amounts of money. Yet financial institutions are capitalistic organizations with a strong emphasis on marketing. Most financial institutions now profiting from EFT owe their success to enormous expenditures on marketing and advertising.[233] This marketing perspective has both general and specific conflicts with privacy. For example, a bank outside Denver uses signature verification terminals, which also provide account information for its tellers. These terminals are manufactured by the inappropriately-named Informer Inc. of Los Angeles. But the bank also uses these terminals to sell more services to customers by reviewing accounts to determine a need for services and by watching for large deposits.[234]

The danger is that banks in particular will ultimately pursue their self-interest first and make confidentiality secondary to the profit motive, except to the extent that their interests and those of customers intertwine. One must only hope that the desire to avoid more government regulation will lead them in proper directions. Richard L. Kattel, Chairman of the Board and President of the Citizens and Southern National Bank of Atlanta furnished an appropriate perspective at the 1977 National Operations and Automation Conference in New Orleans: "There has been some concern that EFTS will lead to the indiscriminate dissemination of personal records. But as you know better than anyone else, the computer records can be made more confidential than they are now.

Nevertheless, we should take the initiative to design and actively support whatever additional changes in systems or legislation are required to be absolutely certain that the confidentiality of our customer records is protected ... and then make certain they know it."[235] A good example of progress through self-regulation would be the action of Citibank of New York in November, 1976 of adding the following clause in its Master Charge card-holder agreement: "Your performance of this agreement may be reported to credit reporting agencies. No one else will be given such information without proper legal process or your prior written approval. We will try to notify you by phone or by mail of a court order in order to give you an opportunity to object to it."[236] The limitation on disclosure without appropriate legal notice is a step forward, especially in the United States, that could well be imitated in Canada.

Kattel's recommendation may be too optimistic about the prospects for self-regulation by financial institutions. The Canadian Task Force on Privacy and Computers in the early 1970s commissioned two studies of regulatory models, which have implications for this current discussion. Both studies were particularly preoccupied with the regulation of the computer industry. Law Professor John Sharp argued that "the best policy would be to have a system of self-regulation of information system operators by the operators themselves on the basis of rules of conduct made or approved by the regulatory body of the federal government. The government involvement could be much reduced should a professional association of information system operators develop strong traditions and full membership."[237] Sharp outlined a code of conduct resembling a code of ethics for the operators of information systems, which would seek to protect the privacy of personal information.[238] Yet despite this advocacy of self-regulation, Sharp emphasized the various inadequacies of this process: "Self-regulation likely possesses serious drawbacks in the privacy field."[239]

The second study of regulatory models reached a similar conclusion that "self-regulation would not constitute the best means of control in relation to the infringement of privacy by the computer industry."[240] The protection of confidentiality may not always be in a firm's self-interest: "We are here dealing with commercial entities for which the profit motive, quite properly, constitutes the raison d'être and primary operational goal."[241] In addition, the public interest may require more protection than the firm requires for its own purposes: "In proposing the sort of controls that may be required to protect confidentiality, we may be asking the computer corporations to do things that are costly and time-consuming for them and for which they get no benefit except the vague concept that they have helped the public interest, whatever that may be."[242] There is also the problem that individuals and institutions may not agree on what data should be kept confidential.

The various recommendations of the Privacy Protection Study Commission in the summer of 1977 have been greeted in some quarters of the American private sector with the predictable claims that government regulations in the interests of personal privacy will produce impractical and expensive requirements.[243] One solution to this perennial dilemma is for industries involved in the development of EFT systems to make their own evaluation of the need for protective measures and implement them. Alan F. Westin told the American Management Association that legislation and regulation for the private sector were avoidable if businesses examined their personal record-keeping practices and voluntarily corrected abuses.[244] One virtue of compliance now with the most predictable and essential needs is that systems will not have to be changed if legislation for the private sector is eventually enacted.

The American Bankers Association has taken the interesting step of retaining the consulting firm of Touche Ross and Co. to do research on the implications of the Privacy Protection Study Commission's recommendations for banks of all sizes. This study is due by the end of 1978.[245] The various professional and trade

associations of Canadian industries involved in the development of EFT systems, such as the Bank Security Committee of the Canadian Bankers Association, could take similar steps to anticipate changes to protect privacy and avoid excessive government intervention. Task forces on privacy for specific financial institutions (using some senior personnel) could evaluate the implications for their own activities of a set of recommendations such as those of the Privacy Protection Study Commission.

IV.b. Provisions for Data Security

In its final report in the fall of 1977, the NCEFT devoted considerable attention to security measures for EFT, including advanced technology and management controls, which are relevant in the Canadian context. The Commission asserted that American regulatory agencies, financial institutions, trade associations, and suppliers of EFT products and services are aware of security vulnerabilities and solutions. They are engaging in a process of education and risk analyses of cost versus the potential for fraud.[246] The Commission concluded on the basis of its expert studies "that while the security of EFT needs to be upgraded continually, technical and procedural solutions to all known security problems are currently available."[247] The IBM study on data security reached the similar conclusion that although there is no such thing as perfect security, at present "most organizations may achieve a level of protection appropriate to their needs."[248] One member of NCEFT criticized the Commission's optimistic approach to the security question. Albert A. Foer claimed that EFT systems are totally vulnerable, which is probably a correct technical statement. Safeguards are available for a price, but they can also be penetrated for a price. Foer urged the creation of a federal EFT security coordinating group as a clearinghouse for security information.[249]

In fact, American federal agencies have developed guidelines for maintaining the security of EFT systems. These guidelines have

not been issued yet so as to give depository institutions opportunities to experiment with various forms of protection.[250] Canadian federal and provincial agencies have either not undertaken or not published the results of similar activities. The Federal Deposit Insurance Corporation in the United States engaged a firm of consultants to prepare a guide to EDP and EFT security based on occupations. This study became a source for the Commission to produce two tables of measures to prevent computer abuse by personnel with access to an EFT system.[251] These tables identify internal fraud control points and internal fraud detection techniques. One significance of these tables for this study is the revelation of the extent to which financial institutions and similar organizations do have the capacity, both managerial and technical, to identify and deal with potential problems with respect to confidentiality and security. The problem is to ensure that such steps are in fact taken in Canada. Protective measures must be included in the initial design of systems, since it is hard to build in security after the fact. At the very least capabilities for security in future stages of development must be initially created, because of cost considerations.

Every Canadian organization involved in EFT, whether governmental or private, should prepare and implement guidelines and standards for the protection of the confidentiality and security of data. Guidelines should solidify the commitment of the financial institution to the appropriate goals. A commitment to confidentiality and security by management should have a major impact on an organization. Managerial reluctance to invest in computer security can be overcome. Programmers can be encouraged to implement provisions for security, in addition to their major and customary preoccupation with making major systems function. Many of the needed controls for computer security are administrative and not technological in character, or else only involve the software.[252] As a matter of policy, the management of financial institutions should restrict the building of interconnected data banks, unless absolutely necessary for the functioning of a

particular segment of an EFT system. Such undertakings pose major technical problems in any event.[253] Westin and Baker set forth a basic principle in recommending the need for "mechanisms to ensure that name-search scanning capacities of the kind falsely attributed to the present American Air Lines reservation system are not installed by managements in a computerized operation unless these are necessary for the organization's operations and proper safeguards against unauthorized or improper use are provided, perhaps with review of these issues by some kind of supervisory agency."[254]

The management of both financial institutions and computer manufacturers must be encouraged to pay more attention to security issues. At its current level of development in Canada in particular, technological solutions exist for most of the confidentiality and security problems presented for EFT. The steps in achieving technical computer security are adequately understood.[255] These include access control through identification, authentication, and authorization, auditing or journaling to monitor systems use, the concealing of information through encryption when confidentiality is important, and hardware security measures.[256] Audit trails built into a system can record every significant communication between a user and a computer.

In recent years and perhaps for obvious reasons, the IBM Corporation has made significant contributions to the subject of data security, even though it rejects the notion that you can prove a system is secure. Its major study of data security identified the following essential elements: management direction; procedures and controls, such as audit controls and the division of responsibilities; physical protection; and computer defenses. The latter include access control by means of identification, verification, and authorization; the promotion of system integrity by isolating users and detecting intrusions; and the use of a

journal or log of computer use to promote accountability.[257] IBM has made its own internal Advanced Administrative System (A.A.S.) a model in the security field. A.A.S. has 16 major marketing applications, 3600 terminals at 400 locations across the United States, and 14,500 terminal users. The daily journals that monitor all requests and inquiries from terminals are kept for a year.

IBM Canada has recently evidenced its concern by appointing a manager for data security programs. One of his early activities was a "Customer Executive Data Security Seminar" in Toronto on December 8-9, 1977. The purpose of the seminar was to generate and sustain data security awareness, to focus on data security techniques, and to plan additional seminars if the response was favourable. The range of topics discussed at the seminar illustrates the level of awareness that already exists in the field of security: risk assessment; data security; a systematic approach; resource access control facility (RACF); encryption; EDP auditing in IBM; signature verification; physical security; and auditing. Similar issues were addressed in cross-country Executive Seminars on data security organized by IBM during the last week of April, 1978.

The IBM topics suggest the wide range of existing and new technologies available for data security. IBM makes available a large number of products to support the needs of customers.[258] Some of the current counter-measures are not widely accepted because of cost and/or reliability. IBM currently has great expectations for the signature verification system of security. It is based on the speed of signature dynamics with which a person signs his or her own name.[259] Experimental research is continuing. IBM has also recently introduced a piece of software to improve control of data security known as RACF, the Resource Access Control Facility. The system creates a profile for each authorized user that contains information for user

identification, verification, authorization, and logging. Canada Trust and the Canadian Imperial Bank of Commerce have purchased RACF.

A seemingly futuristic proposal attempts to deal with the question of the security of the data entry card in an EFT system. It is possible to introduce into the plastic card a random property or radioactive isotope. This random property is read optically or magnetically. The randomness is virtually impossible for a counterfeiter to reproduce. Radioactive materials are supposed to be harmless in low quantities, controlled, and not readily available.[260]

The most generally available solution to the vulnerabilities of computers and the need to protect confidentiality is the enciphering and deciphering of data.[261] Although encryption is said to be only moderately expensive, the NCEFT concluded that "there is no evidence... in terms of losses sustained, that encryption is presently economically justified."[262] IBM has recently developed a coding system (algorithm) for encryption, which was published in 1977 as the new Federal Encryption Standard by the National Bureau of Standards in the United States.[263] The relevant equipment, which is a small box that can be attached to a computer, is known as the Data Encryption Standard (DES). DES has its own key to encode and decode data and is very simple to set up. Each user of the equipment generates its own key. Despite criticisms by some companies, such as the Bell Telephone system in the United States which argues that DES is too insecure to use, a major American bank, Citibank, plans to implement DES and considers it a step forward. Much of the criticism revolves around the capacity of a government organization, such as the National Security Agency in the United States, to build an expensive machine to determine any user's unique key in DES.[264]

The problem of identifying customers is a particular issue in EFT. The use of a personal identification number (PIN) is

the current solution, but "technologies are being developed for more secure identifiers, such as electronic signature verification"[265] Professor C.C. Gotlieb of the University of Toronto, a computer expert, says that voice prints may be the answer to the problem of authorization and identification in EFT. Voice prints are as individual as fingerprints and could easily be made machine-readable.[266] IBM testing has found voice prints to be unreliable because of the varying qualities of transmission lines in carrying sounds. Expense is also a factor in voice recognition systems, but this may change over time as data processing becomes cheaper and cheaper. In a similar manner encryption should be used selectively at present because of the cost involved, but is becoming more cost effective.[267]

The question remains whether legislative intervention will be necessary to ensure data security. There are two segments to the problem: financial organizations need to be encouraged to promote security and confidentiality in EFT, and public sanctions have to be created for breaches of security. The Westin and Baker study of record-keeping in various types of organizations in the early 1970s found that organizations were not convinced of the risk of unauthorized access and thus instituted few provisions for protection: "The strong impression that we drew at our site visits was that whether organizations would give the staff attention, spend the money, and accept the constraints on system operations that security measures generally require will depend primarily on outside pressures, especially the attitudes of regulatory agencies and lawmakers on how important it is to ensure confidentiality of information in various sectors of record-keeping."[268] While financial institutions have strong internal incentives towards confidentiality and security, even the National Commission on Electronic Fund Transfers, which appears to have been industry dominated, concluded that uniform state and federal regulation was necessary in the security field, especially to strengthen federal criminal codes against misuse of computer

systems.[269] Thus the need for statutory deterrence seems established. Even large investments in security by relevant organizations can only reduce the risk of penetration; large-scale interconnected financial and marketing systems will remain vulnerable to the terrorist and the thief.[270]

In the United States, the Bank Protection Act of 1968 is the principal legislation requiring federal financial supervisory agencies to promulgate standard rules for security devices and procedures to discourage robberies, burglaries, and larcenies.[271] Legislation more directly relevant to EFT is now pending. In the last Congress Senator Abraham Ribicoff introduced a bill known as "The Federal Computer Systems Protection Act of 1977." It would become the first federal law aimed directly at controlling computer-related crime, especially in banking systems ensured by the federal government.[272] Hearings are scheduled on Senate bill 1766 in 1978. The draft bill simply adds a very simple provision against computer fraud to the U.S. Code. The bill is designed to control unauthorized access to a customer's EFT account by theft or reproduction of a card, unauthorized access by personnel running an EFT system, such as store employees, unauthorized access to communication lines, and unauthorized access occurring at a central processing unit.[273] Another piece of pending legislation, the Bill of Rights Procedures Act, would extend the laws against wiretapping to computer data transmissions.[274]

IV.c. Statutory Remedies

The Need for Legislation

There appears to be general agreement in the United States that some legislation is required to regulate EFT systems. The American Civil Liberties Union's Privacy Report concluded its review of EFT by determining that the first need is "the provision of a strong statutory basis for the protection of personal privacy both under present financial structures and under an EFT system."[275] In the United States, various commentators, including the Privacy

Protection Study Commission, have also concluded that legislation is necessary for the protection of privacy, confidentiality, and security.[276] Legislators, with ultimate assistance from the courts may be in the best position to settle the appropriate balances between individual and public interests in financial records and EFT. The NCEFT has accepted the need for limited regulation at least in connection with consumer issues.[277] The Commission did not think it appropriate at this stage to create a massive new structure of regulation for EFT or computer security.[278] On general issues connected with EFT the Commission concluded that the evolutionary development of such systems in the United States and other industrialized countries means that various levels of government "are in a position to monitor developments and act in time to protect the public interest if adverse effects appear."[279]

Nevertheless in the area of privacy protection in particular, the NCEFT did identify the need for federal legislation to control government and third party access to consumer financial information.[280] "Although a legal framework governing EFT transactions is evolving through private contract, additional publicly-established consumer rights and protective measures are desirable. Hence, the Commission's primary effort in this area has been to suggest guidelines for a legal framework and service characteristics that must govern the rights, responsibilities, and liabilities of participants in the new payment system."[281] The basic elements in this American analysis are worth highlighting because of their potential relevance in Canada: the role of private contract, the need for a legal framework in public law, and the need for good service characteristics. The NCEFT suggested that legislation protecting personal privacy must also take into account the legitimate needs of law enforcement agencies, the legitimate uses of information gathered by financial institutions, and governmental needs for access to financial information.[282]

A number of Canadian commentators and organizations have similarly concluded that there is need for federal and provincial

legislation to protect personal privacy and related values in connection with computerized data banks and EFT. Ten years ago the then chairman of the Ontario Law Reform Commission, H. Allan Leal, was of the opinion that "a system of licensing data banks and their operating personnel, the provision of standards, and the periodic inspection of their operation are the only means by which excesses can be prevented."[283] Another commentator favoured the regulation of data banks and data transmission technology.[284] Professor Peter T. Burns, who studied the Canadian law of privacy, concluded that "it cannot be too strongly argued that regulation of all systems of computers concerned with personal information is a vital step in the direction of privacy preservation."[285] The federal government's position paper on EFT in 1975 concluded that the federal government should protect consumer's rights, including the right of privacy: "Questions of privacy need to be addressed in the context of the government's general policy now being developed on the computer and privacy. In most cases it will be necessary to prevent access to account status information except for legitimate authorization inquiries with the consent of the account holder."[286] The Justice Department has been instructed to take the lead in furnishing a response for the federal government to the legal and consumer issues raised by EFT. There have been no public indications that such initiatives are bearing fruit.

Professor John Sharp in the early 1970s studied various regulatory models in connection with the Task Force on Privacy and Computers. His study discussed the protection of privacy through regulation of the information industry by a federal regulatory board controlling both operators and owners of information systems.[287] He wisely emphasized that "privacy policies designed to protect computerized data must be integrated with communications policy and the criminal law."[288] He particularly favoured licensing of private information systems by a federal government agency.[289] This would be comparable to the role of the Swedish Data Inspection Board under the Data Act.

Sharp's proposals to control owners of an information system would include certification, inspection, bonding, malpractice insurance, the hearing of complaints, and the imposition of sanctions and penalties. Given the conservative characteristics of the development of data protection legislation on the international level, including Canada, it seems unlikely that the time is now ripe for such an expansion of jurisdiction into the private sector.

Sharp pointed out that overall policy for the protection of privacy in Canada, especially with respect to computerized data, requires cooperation between federal and provincial authorities.[290] The federal government has already taken measures to regulate federal data banks through the provisions in Part 4 of the Canadian Human Rights Act of 1977. The federal government has a number of statutes regulating telecommunication common carriers, which may be useful in this respect.[291] The draft federal Telecommunications Act could easily address issues of confidentiality.[292] The federal Railway Act does regulate various common carriers as telecommunications companies, but mostly in connection with rate regulation and not confidentiality.[293]

Other federal statutes, such as the Bank Act, should address issues of privacy, confidentiality, and security now that EFT systems are being developed. The Bank of Canada, the Minister of Finance, and the Inspector General of Banks are also in a position to regulate chartered banks in the interests of such values. Although the current Bank Act (a revision is expected in Parliament in 1978) does not address the issue of confidentiality, such a provision was included in the first Bank Act in 1871 to about the time of the First World War. For example, the Bank Act of 1890 stated that "the books, correspondence and funds of the bank shall, at all times, be subject to the inspection of the directors; but no person, who is not a director, shall be allowed to inspect the account of any person dealing with the bank."[294] An updated version of the law on confidentiality and disclosure should be

inserted in the Bank Act. The draft Borrowers and Depositors Protection Act from the federal Ministry of Consumer and Corporate Affairs could similarly include stronger protections for the confidentiality of customer data. One section in the draft Bill prohibits "conduct involving the unreasonable publication or communication of information in relations to a lending transaction or to a borrower."[295]

The province of Ontario would appear to have potential regulatory power over financial transaction data. The Loan and Trust Corporations Act authorizes the Lieutenant Governor in Council to make regulations for various aspects of the operations of loan and trust companies, which could conceivably be used to protect the interests of depositors in privacy and confidentiality.[296] The potential regulatory power of the Ontario government is even stronger for credit unions. The statute authorizes the Lieutenant Governor in Council to make regulations "governing the operations and powers of branches of credit unions," "governing credit unions and leagues of credit unions," and "prescribing any matter required by this Act to be prescribed by the regulations."[297] In the regulation of developing EFT systems the province of Ontario could also strengthen the provision in the Consumer Protection Act that requires the written acceptance by credit-card users of the terms of the arrangement.[298] The government should restrict the extent of contracting-out of personal rights, which individuals are frequently obliged to accept. Finally, the province has limited jurisdiction in the field of telecommunications. The Ontario Telephone Service Commission has some regulatory power over common carriers in the telecommunications field.[299] The Ontario Telephone Act prohibits divulging a "message" acquired from a telephone line, which could be applicable to developing EFT systems.[300]

The Content of Legislation

Legislation to preserve the privacy, confidentiality, and security of financial information in EFT systems should cover a

variety of items. Government operation of essential elements in an EFT network should be avoided, if possible. In the United States, the Privacy Protection Study Commission recommended "that no governmental entity be allowed to own, operate, or otherwise manage any part of an electronic payments mechanism that involved transactions among private parties."[301] This recommendation was in response to the potential of EFT data for government surveillance, which poses "an unparallel threat to personal privacy."[302] However, the NCEFT disagreed with the Privacy Commission on this point, primarily because the Federal Reserve already operates automated clearinghouse facilities. The NCEFT was satisfied with the provision of stronger controls on access to data in the hands of this Federal Reserve system.[303] This issue can be avoided in Canada, if the proposed single EFT network is run by the Canadian Payments Association as an independent entity.

Regulation of EFT should, in particular, control the scope of data collection and retention. It is absolutely crucial to regulate the input of data into the process. The Privacy Commission recommended restrictions on the collection of identifiable information and its retention in the switching mechanisms of EFT for at most a limited period.[304] The NCEFT agreed that "transaction records should be maintained by the switch only for the period of time necessary to resolve disputes -- perhaps a few months. After that time, there is no operational motive for the switch to store them, and such records should be destroyed."[305] This Commission also recommended the adoption of federal legislation "to ensure that to the extent that the merchant is unaffected as to cost or risk, the type of transaction that the customer's EFT card triggers at the point of sale should be confidential between the customer and his depository institution."[306]

Controlling the dissemination of EFT data is one of the most crucial areas of regulation. At the time of initial involvement with financial institutions and EFT systems, customers should

be fully informed about intended uses of data. As a general principle, the consent of the customer should be required for any non-routine uses of such information.[307] Although controls on government access to such data should take account of fundamental needs of law enforcement agencies, an individual consumer should have the right to contest government access to data.[308] Equally strict controls should exist for the dissemination of EFT data to third parties in the private sector. Such regulation of disclosure to third parties should take account of the needs of the operators of the system and make it possible for a customer to consent to the release of data.[309] At the very least the rights of access to data banks by government agents and third parties should be controlled by legal process. As will be discussed further below, restricting the use of EFT data for surveillance purposes requires various types of sanctions and monitoring devices to discover violations.

Another possibility worth exploring in Canada is a change in the prevailing law concerning the ownership of personal data in financial institutions and EFT systems. Robert E. Smith, the publisher of the Privacy Journal, has recommended the development of the principle that an individual owns his own data.[310] Alan F. Westin has proposed that a person's data profile in an EFT data base ought to belong to the person as private property and not to the system.[311] In the United States cancelled cheques and possibly deposit slips and debit memos are the property of the depositor under the common law; the bank holds these documents as agent for the depositor. The Privacy Protection Study Commission concluded that "a common-law standard is beginning to emerge in the States which suggests that banks act as mere agent in their handling of account information for depositors, and that, in essence, the account information is more the depositor's than the banks."[312] But, "most government searches are of microfilms and photocopies, items which, unlike the originals, are the bank's property."[313] There has been little

litigation on this point since the concept of a property right was established in nineteenth-century cases. A new problem now arises since "an electronic funds transfer system... would eliminate all vestiges of property owned by the depositor, ... despite the fact that no basic change in the character of the relationship between depositor and bank has occurred."[314]

The Right of Privacy

Although the common law right of privacy is better developed in the United States than in any other Anglo-American jurisdiction, the above discussion has shown that the federal common law right of privacy has little utility in the area of financial and EFT records. The United States Supreme Court seems to have specifically rejected the establishment of a right of privacy for financial matters. The search and seizure provisions of the Fourth Amendment have yet to benefit American litigants in such cases.[315]

The common law right of privacy is even less developed in federal and provincial jurisdictions in Canada than in the United States. Professor Peter T. Burns has concluded in connection with the common law protection of privacy that "there is little chance of a body of coherent rules being developed. Instead the legislators must be regarded as the bodies to turn to if privacy as a vital social state is to be reinforced by legal action."[316] Privacy statutes in Canada are similarly underdeveloped. At the federal level a section of the Human Rights Act regulates federal government data banks and a misnamed "Protection of Privacy Act" regulates wiretapping.

The federal Human Rights Act has some potential for suggesting the future thrust of data protection legislation in Canada. The basic principle of the Act is that "the privacy of individuals and their right of access to records containing personal information concerning them for any purpose including the purpose of ensuring accuracy and completeness should be protected to the

greatest extent consistent with the public interest."[317] Individuals are granted various "entitlements" in furtherance of the above principle.[318] The concept of appropriate uses of data is also suggestive of EFT-type applications. A derivative use is "use of a record for a purpose consistent with the use for which it was compiled."[319] Derivative uses of information must be published; the consent of the individual is required for non-derivative uses.[320] The Human Rights Act also provides for a Privacy Commissioner, whose task is to receive and investigate public complaints.

Three Canadian provinces have passed Privacy Acts, which seem to have had negligible impact, use, and development.[321] Their main virtue is the establishment of a general right to personal privacy. The prototype was the British Columbia Privacy Act of 1968, which determined that "it is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another."[322] The same provision occurs in the 1974 Saskatchewan Privacy Act.[323] The Manitoba Privacy Act of 1970 states that "a person who substantially, unreasonably, and without claim of right, violates the privacy of another person, commits a tort against that other person."[324]

The state of Canadian privacy legislation suggests that there is little hope of relying on existing Canadian cases and legislation to protect the privacy of individuals injured by the release of financial information. Professor John Sharp concluded that "the absence of privacy legislation in most of Canada, the truth defense to a defamation action, and the uncertainties in the application of doctrines of negligence, confidentiality or proprietary rights can be formidable barriers to the party injured by a disclosure of personal data."[325] Sharp argues the need for stronger means to protect individuals from the threat of new technologies, which would include EFT. The division of constitutional jurisdiction to protect privacy between the provinces and the federal government requires careful study.[326]

Since a number of western Canadian provices and Quebec have enacted simple statutes for the protection of personal privacy, the creation of a statutory right to personal privacy in Ontario would appear to be a high priority. A Commission on Freedom of Information and Individual Privacy is currently studying government data practices in Ontario. Deputy Attorney General H. Allan Leal recently stated to this Commission that "the concept of a right of individual privacy remains essentially unrecognized at law in Ontario. Privacy protective measures do exist in a number of Ontario Statutes. These provisions too have been introduced on an ad hoc basis and reflect a policy vacuum."[327] Leal indicated the desireability of enacting a "Government Information Practices Act" declaring the intention of the Ontario legislature to foster freedom of information and protection of privacy.

Developments in other jurisdictions with legislation on privacy and data protection suggest that such developments will ultimately lead to the private sector. A privacy statute could include various types of protections for financial data in banking and EFT transactions. The recent development at the federal level and in Ontario of the concept of the ombudsman may also have some merit in terms of protecting individuals from alleged abuse. The Privacy Commissioner created under the Canadian Human Rights Act will become a part of the new federal ombudsman's office, after appropriate legislation is enacted. It seems likely that the jurisdiction of the federal privacy ombudsman will increase as the pressure for more and more data protection grows and is recognized.

Financial Information Privacy Acts

In terms of protecting the confidentiality of financial transaction information, the model of the American right to financial privacy acts may be of more direct utility for Canada and Ontario than general privacy legislation. The California Right to Financial Privacy Act of September 28, 1976, which has

been discussed in detail above, is the explicit model in this connection. Maryland and Illinois have also recently passed laws on financial privacy.[328]

A number of efforts are currently underway to pass federal financial privacy legislation in the United States. The proposed legislation, which covers all financial institutions, has been approved by the American Bar Association, the American Bankers Association, and the American Civil Liberties Union.[329] Despite formidable opposition from law enforcement agencies, this federal legislation gives the customer specific rights to know of and contest government attempts at access to personal financial data. A customer's consent to release data must be for specific information, of limited duration, and revocable. A customer is also entitled to injunctive relief and actual and punitive damages.[330] Such conditions and restrictions are along the lines of the recommendations of the NCEFT for controlling access to financial information for law enforcement.[331] A member of the Commission, Albert A. Foer, prepared his own format for a consent form for the release of data to third parties, which is a much tougher formulation than the one proposed by the entire Commission.[332] The applicability of such American federal models as the Fair Credit Reporting Act of 1970 to the new problems posed by EFT financial transactions should be further studied in the Ontario and Canadian context.[333]

Another effort at federal legislation to protect financial privacy is the Bill of Rights Procedures Act (BRPA), which was re-introduced in the House of Representatives in 1977.[334] This bill presents a refined balance between the legitimate needs of law enforcers and the privacy interests of bank customers. It provides statutory protection for individuals from government surveillance. Title 1 limited government access to records kept by financial institutions. BRPA provides for four methods to authorize federal government access to bank records. Three involve

legal process and the fourth involves direct customer authorization. Any other disclosure of customer information by banks to agents of the government is made illegal. The proposed bill also provides for notice to customers of government intent to obtain access to their data. The only exception to the requirement for notice occurs in connection with the jeopardization of a serious criminal prosecution or the committing of a serious criminal offense.[335] The relatively weak remedies section of the BRPA bill will be discussed further below.

EFT Statutes

The limitations of various American state EFT laws in connection with the protection of privacy, confidentiality, and security have already been discussed above. With a handful of notable exceptions, these state laws pay insufficient attention to the protection of these various values. The need for additional protections for consumers is almost self-evident in every state EFT statute and should be included in any future Canadian legislation.

In addition to the proposed bills discussed in the previous section, a number of efforts are underway at the federal level in the United States to pass what could be termed EFT statutes. Senate bill S.1766, "The Federal Computer Systems Protection Act of 1977," which has been discussed previously, provides for criminal penalities for computer fraud.[336] Senator Thomas J. McIntyre (Democrat-N.H.), Chairman of the Senate Banking Subcommittee on Financial Institutions, has introduced a trial EFT bill, which provides for no access by any level of government to a customer's financial records without the consent of the customer or appropriate legal process.[337]

Senator Donald W. Riegle, (D. Michigan), Chairman of the Senate Consumer Affairs Subcommittee, has introduced another bill on EFT to limit access to financial account information by third parties.[338] Senate Bill X.2065 is known as the "Electronic Fund

Transfer Consumer Protection Act."[339] The purpose of the bill is "to provide a basic framework establishing the rights, liabilities, and responsibilities of all participants in electronic fund transfer systems."[340] The primary objective, however, is the protection of individual consumer rights. The bill provides for the issuance of regulations by the Board of Governors of the Federal Reserve system to carry out the purposes of the act. Financial institutions are required to disclose fully the terms of EFT accounts to consumers, including "the financial institution's fiduciary duty to protect the consumer's right to privacy and assure the integrity, accuracy, and security of the consumer's account under Section 816."[341] A major section of the proposed bill concerns the fiduciary duty of financial institutions:

> A financial institution shall be deemed to have a fiduciary duty to each consumer for whom it effects electronic funds transfers to ensure the security, integrity, accuracy, and confidentiality of each account of the consumer accessible by means of such transfers. This duty includes -
>
> 1) notifying the consumer as soon as possible of any action against the consumer's account;
>
> 2) designing all mechanisms, means, and systems employed in effectuating electronic fund transfers to prevent unauthorized electronic fund transfers and to detect and correct such transfers;
>
> 3) preventing information regarding any electronic fund transfer from being disclosed to any person other than -
>
> a) the consumer making the transaction;
>
> b) any other person who is a party to the transfer or is necessary to effectuate the transfer, but only to the extent that the information disclosed is necessary to effectuate the transfer;
>
> c) those persons authorized by law to have access to the records of the financial institution or of the parties to the transactions; and

d) any other person specifically authorized in writing by the consumer to receive such information; and

4) meeting any other duty of a fiduciary nature recognized or imposed by state law.[342]

The civil and criminal liability provisions of this bill will be discussed further below.

Enforcement Mechanisms: Civil and Criminal Liability

Legislation providing for the privacy, confidentiality, and security of financial transaction information should provide for civil and criminal liability for breach of duty. In particular, the liability of financial institutions and their employees for the unauthorized disclosure of customer information must be established. The imposition of liability in this manner would be an important step in self-regulation for financial institutions and computer companies.

The American NCEFT produced a set of guidelines as a basis for a model EFT consumer code. Since in the United States banks are responsible for the unauthorized use of cheques, unless negligence can be proven, the Commission sought a similar assignment of liability to depository institutions under EFT.[343] The recommended approach of the Commission "places the liability for errors and fraud squarely upon the depository institutions. It creates a strong incentive for depository institutions to use the most secure technology for customer identification, because the institution would be liable when a stolen card and the customer identification code (obtained, for example, by observing the customer at a terminal) is used within a short time after the theft of the card. Further, because the depository institution -- not the consumer -- is liable for fraud such as "computer crime" or tampering with the data base of any sort,

there is further incentive to use the [most] cost-secure technology possible."[344] The Final Report of the Commission recommended federal legislation to give consumers a right to recover damages for injuries suffered as a result of the violation of the consumer protection provisions recommended by the Report.[345]

Several studies and reports have established the desire of consumers for rights of redress in the form of damages if the confidentiality of their financial information is abused by EFT.[346] The Florida and Iowa EFT laws establish the liability of the financial institution for unauthorized transactions.[347] The federal Bill of Rights Procedures Act of 1977 provides weak remedies for the unauthorized disclosure of bank customers' financial information. The bill limits monetary recovery to actual damages, and, if a wilful violation is established,punitive damages. A critic has noted that "actual damages for the violation of the privacy of one's bank account are extremely difficult to prove since the value of privacy is not easily measured in monetary terms. In order to provide effective sanctions, the bill should contain a liquidated damages provision, similar to that found in the Privacy Act of 1974."[348]

Senator Riegle's proposed Electronic Fund Transfer Consumer Protection Act provides for criminal liability for anyone who knowingly and wilfully fails to comply with any provision of the bill. The maximum fine is $5,000 or imprisonment for not more than one year.[349] Civil liability is imposed on any person who fails to comply with any provision of the bill with respect to any consumer.[350] Civil liability is restricted primarily to actual damages sustained by a consumer as a result of a failure to comply with the bill. Restrictions are seemingly imposed on the damages for which a particular person might be liable. Class actions are also permitted.

Canadian financial institutions are probably liable for the release of confidential information to a third party without the customer's consent.[351] The real issue is the extent to which financial institutions and their employees should be held civilly or criminally liable for unauthorized disclosures of confidential information. Professor Sharp's study of regulatory models for the computer industry in Canada advocated the imposition of strict civil liability by provincial statute and the imposition of penal sanctions on the system or the operator under the federal criminal code.[352] In his view the law of tort should control the majority of abuses of computerized data, and the criminal law should be used only for the most serious invasions of privacy.[353] Sharp favors strict civil liability "as the means of protecting the public from the effects of harmful disclosure of personal, confidential information, by data banks."[354] Sharp suggests that a civil action for breach of duty should be actionable without proof of damage, and describes conditions that should exist for a plaintiff to succeed in an action under the doctrine of strict liability.[355]

V. RECOMMENDATIONS

Financial Institutions

1. Publicly affirm and maintain the highest standards of confidentiality for customer data and financial transaction information.

2. Draw up and implement basic rules and regulations for the collection, protection, and disclosure of personal information and financial transaction data.

3. Draw up and implement voluntary industry guidelines for the confidentiality and security of customer data and financial transaction information. The Directors of a financial institution should require their internal audit department to certify that their institution is in compliance with the guidelines.

4. Implement measures to restrict unauthorized access to customer data and financial transaction information by employees of financial institutions, including training programs and monitoring.

Governments

1. Raise the consciousness of financial institutions and the computer industry with respect to concern for privacy, confidentiality, and security by publishing the contents of this Working Paper.

2. Continue to monitor the development of EFT systems in Canada in order to protect the interests of citizens in the privacy, confidentiality, and security of their personal data.

3. Promote the preparation of voluntary guidelines, standards and regulations for the protection of confidentiality in the operation of personal data systems in the financial field. The model guidelines prepared by the Privacy Committee of New South Wales in April, 1977 are exemplary in this connection.

4. Consider the enactment of a statutory right to financial privacy along the lines of the California, Illinois, and Maryland models, which would mandate confidentiality for financial transaction information, control third party access to customer data, require notice to customers of requests for access by third parties, limit the scope of data collection, and establish statutory minimum damages at a significant dollar amount for breach of duty by unauthorized disclosure of personal financial data.

5. Reinforce the existing implied contract between financial institutions and customers/depositors by a statutory provision to prohibit contracting out of information rights and to design proper releases for individuals to sign when entering into financial relations with financial institutions.

6. Grant customers of financial institutions a property interest in their financial transaction information.

F O O T N O T E S

1. See Alan F. Westin, Privacy and Freedom (N.Y., 1967), Part One; and David H. Flaherty, Privacy in Colonial New England (Charlottesville, Va., 1972), pp. 1-13.

2. Information Hotline, IX (Oct., 1977), 9.

3. Privacy Protection Study Commission, Personal Privacy in an Information Society. Report of the Privacy Protection Study Commission, (Washington, D.C., 1977), pp. 6-21. (hereafter cited as PPSC, Personal Privacy in an Information Society).

4. California Bankers Association v. Shultz, 94 S. Ct. 1494 (1974), at p. 1529.

5. Stephen M. Ege, "Electronic Funds Transfer: A Survey of Problems and Prospects in 1975," 35 Maryland Law Review (1975): 54-55.

6. The Privacy Report, V (October, (1977), p. 3-4.

7. National Commission on Electronic Fund Transfers, EFT and the Public Interest (Washington, D.C., February 1977), p. XII (hereafter cited as NCEFT, EFT and the Public Interest).

8. Ibid., P. XII.

9. For a general review of consumers' concerns for privacy and EFT, see the article by William O. Adcock and Anne M. Moore of Payments Systems Inc. in Computerworld, X, No. 37, (September 13, 1976), p. 25.

10. See Silver Donald Cameron, "Between Heaven and Orwell," Toronto Globe and Mail, Weekend Magazine February 26, 1977, pp. 4-7.

11. Herbert A. Simon, "What Computers Mean for Man in Society," Science, Vol. 195 (March 18, 1977): 1190.

12. National Commission on Electronic Fund Transfers, EFT in the United States, Policy Recommendations and the Public Interest (Washington, D.C., October 28, 1977), pp. 186-187. (hereafter cited as NCEFT, EFT in the U.S.).

13. Y. Abe, "A Japanese On-Line Banking System," Datamation (September, 1977): 89-97.

14. Computer Data, II, No. 10 (October, 1977).

15. Bank of Montreal, Annual Report 1977, pp. 4, 12-13.

16. Paula S. Mitchell, "Electronic Funds Transfer Technology. A Canadian Perspective Working Paper," (December 22, 1977), pp. 5-6. (hereinafter cited as Mitchell, "EFT Technology.")

17. Computer Data, II, No. 10, (October, 1977).

18. Toronto Globe and Mail (June 11, 1977), p. B1.

19. Computer Data, II, No. 10 (October 1977), No. 143.

20. Mitchell, "EFT Technology," p. 20.

21. Ibid., pp. 23-24.

22. Privacy Report, V, No. 3 (October, 1977), p. 3-4.

23. Privacy Protection Study Commission, Technology and Privacy (Washington, D.C., 1977), p. 20. (hereafter cited as PPSC, Technology and Privacy).

24. Ibid., pp. 24-25.

25. Alan F. Westin and Michael A. Baker, Databanks in a Free Society (New York, 1972), p. 129.

26. NCEFT, EFT and the Public Interest, p. 24.

27. NCEFT, EFT in the U.S., pp. 7, 20-23.

28. Ibid., pp. 20-23.

29. See Note (Peter J. Shurn), "Electronic Funds Transfer Systems: A Need for New Law?" 12 New England Law Review (1976): 118-119.

30. Sanford Rose, "Checkless Banking is Bound to Come," Fortune (June, 1977): 126.

31. Advisory Committee on Automated Personal Data Systems. Records, Computers, and the Rights of Citizens. (Washington, D.C., 1973) ch. 2.

32. Note, "Government Access to Bank Records," 83 Yale Law Journal (June, 1974): 1441.

33. Mitchell, "EFT Technology," p. 25.

34. Harry Kalven, Jr., "The Problems of Privacy in the Year 2000," in Daniel Bell, ed., Toward the Year 2000. Work in Progress (Boston, 1968), pp. 245-246.

35. PPSC, Personal Privacy in an Information Society, p. 116.

36. See Comment, (Elaine Block Davis), "Government Access to Bank Records in the Aftermath of U.S. v. Miller and the Tax Reform Act of 1976," 14 Houston Law Review (March, 1977): 636 note. (hereafter referred to as Comment "Government Access to Bank Records," 14 Houston L.R. (March, 1977).

37. For a sample, see Computers and People, (August, 1975): 31-2.

38. Blair C. Shick, "Privacy - the Next Big Issue in EFT," 68 Banking (March, 1976): 74.

39. PPSC, Personal Privacy in an Information Society, p. 118.

40. James B. Rule, Value Choices in Electronic Funds Transfer Policy (Washington, D.C.: Office of Telecommunications Policy, (October, 1975), p. 23.

41. PPSC, Personal Privacy in an Information Society, p. 120.

42. NCEFT, EFT in U.S., p. 187.

43. Mitchell, "EFT Technology," p. 61.

44. NCEFT, EFT in U.S., p. 338-339.

45. Computerworld XI, No. 49, (December 5, 1977): 39.

46. PPSC, Personal Privacy in an Information Society, p. 119.

47. H.H. Binhammer, Innovation and Change: Deposit Taking Institutions (Econ. C. of Can., 1976), p. 127.

48. National Commission on Electronic Fund Transfers, Retail Point of Sale Terminals, (Washington, D.C., 1977), p. 7.

49. NCEFT, EFT in U.S., p. 22.

50. NCEFT, EFT and the Public Interest, p. 79.

51. CBA, Factbook, 1977-78, pp. 7-8.

52. Canada, Towards an Electronic Payments System (1975), pp. 7, 14.

53. H.H. Binhammer, Canadian Banker Vol. 84, No. 5 (September-October, 1977): 5.

54. Canada, Towards an Electronic Payments System (1975), p. 24.

55. Toronto Globe and Mail (January 17, 1975), p. 6.

56. Canada, Towards an Electronic Payments System (1975), pp. 18-19.

57. See Eamonn Fingleton, "Banks Without Cash," The Spectator (March 11, 1978), p. 14.

58. National Commission on Electronic Fund Transfers, A Collation of Poll Results and Other Data on Consumer Reactions to EFT (Washington, D.C., October, 1977).

59. In fact, a protective system of this type can be devised if the potential invaders are forced to function from a remote location outside the computer installation. The quotation is from Seymour F. Thompson, "The Invasion of Privacy and Electronic Fund Transfer Systems: Spotlight on Invaders," Computers and People (September, 1976), p. 19.

60. Silver Donald Cameron, "The Death of Money," Quest (November, 1977), p. 25.

61. Ibid., p. 26.

62. Ibid., p. 30.

63. NCEFT, EFT in the U.S., p. 24.

64. Ibid., pp. 257-258.

65. James B. Rule, Value Choices in Electronic Funds Transfer Policy (Washington, D.C.: Office of Telecommunications Policy, October, 1975), p. 25-33.

66. Note "Government Access to Bank Records," 83 Yale Law Journal (June, 1974): 1441-1442.

67. PPSC, Personal Privacy in an Information Society, p. 349.

68. PPSC, Technology and Privacy, p. 30.

69. See the discussion and evidence in Comment, "Government Access to Bank Records," 14 Houston L.R. (March, 1977): 649.

70. Stephen M. Ege, "Electronic Funds Transfer: A Survey of Problems and Prospects in 1975," 35 Maryland Law Review (1975): 54.

71. NCEFT, EFT in the U.S., p. 184: for a general discussion of security in EFT, see Ibid., pp. 183-194.

72. Ibid., p. 186-188.

73. IBM, Data Security and Data Processing Vol. 1, Data Security Site Publications, GBOF - 1200, p. 8.

74. CBA, Factbook, 1977-78, pp. 4, 6.

75. Computer Data, II, No. 10 (October, 1977), No. 140.

76. Stephan Kogitz, "Privacy and Data Security: The DP Manager's Viewpoint," Canadian Datasystems (March, 1978), p. 37.

77. See Toronto Globe and Mail (January 23, 1978), pp. 1-2.

78. Graham Davies, "Computer Fraud. The Crime Companies Won't Report," Financial Times of Canada (November 21-27, 1977), pp. 1,4.

79. Ibid., p. 5.

80. NCEFT, EFT in the U.S., p. 183.

81. Alan F. Westin and Michael A. Baker, Databanks in a Free Society (New York, 1972), pp. 306 and 314.

82. Thomas Whiteside, "Annals of Crime: Dead Souls in the Computer," The New Yorker (August 22, 1977), pp. 35 ff., and Ibid. (August 29, 1977), pp. 34 ff., and Donn B. Parker, Crime by Computer (New York, 1976).

83. Harvey Saul Gellman. Electronic Banking Systems and Their Effects on Privacy. A study by the Privacy and Computer Task Force (Ottawa, 1972), p. 19.

84. Other important consumer issues such as responsibility for errors or negligent misstatements are not discussed in this Working Paper, since they do not impinge directly on privacy and confidentiality.

85. Some of the consumer advantages of EFT are discussed in Sanford Rose, "Checkless Banking is Bound to Come," Fortune (June, 1977), p. 118.

86. PSI Newsletter, Vol. 9, No. 12 (December, 1977).

87. Bank of Montreal, Annual Report 1977, p. 11.

88. PSI Newsletter , Vol. 9, No. 10 (October, 1977), pp. 4-5.

89. PSI Newsletter, Vol. 9, No. 11 (November, 1977), p. 10.

90. PSI Newsletter , Vol 9, No. 10 (October, 1977), p. 10.

91. Silver Donald Cameron, "The Death of Money," Quest (November, 1977), p. 33.

92. NCEFT, EFT and the Public Interest, p. 7.

93. This theme was developed by the Commissioner of Michigan Financial Institution at U.S. Senate Hearings in 1976; see NCEFT, EFT and the Public Interest, p. 8.

94. Information Hotline (June, 1977), p. 7.

95. NCEFT, EFT in the U.S., p. 266.

96. Note, "Government Access to Bank Records," 83 Yale Law Journal (June, 1974): 1463-1464.

97. Alan F. Westin and Michael A. Baker, Databanks in a Free Society (New York, 1972), p. 112. Legal developments since this statement was written will be reviewed below.

98. J.M. Carroll, J. Baudot, C. Kirsh, and J. Ivan Williams. Personal Records: Procedures, Practices and Problems, A Study for the Privacy and Computer Task Force, (Ottawa: Departments of Communications and Justice, 1972), p. 99.

99. Silver Donald Cameron, "The Death of Money," Quest (November, 1977), p. 33.

100. Harvey Saul Gellman. Electronic Banking Systems and Their Effects on Privacy, A Study by the Privacy and Computer Task Force (Ottawa, 1972), p. 2.

101. Bank of Montreal, Policies and Procedures Manual, 35-715-7.

102. Bank of Montreal Form 7483.

103. Bank of Montreal, "Welcome," p. 10.

104. CBA, Factbook, 1977-78, p. 9.

105. Ibid., p. 8.

106. California Bankers Association v. Shultz, 94 S. Ct. 1494 (1974) at p. 1531.

107. Ibid., p. 1534. The last sentence was a particular reference to the requirements of The Bank Secrecy Act of 1970.

108. Privacy Report, "Financial Records," The Privacy Report, IV, No. 3 (October, 1976), pp. 2-5.

109. 94 S. Ct. 1494 (1974), at p. 1515, note 26.

110. Note, "Government Access to Bank Records," 83 Yale Law Journal (June, 1974): 1464 note.

111. Note (Catherine Carl Wakelyn), "Bank Recordkeeping and the Customer's Expectation of Confidentiality," 26 Catholic University Law Review (1976): 93-94.

112. Comment, "Government Access to Bank Records," 14 Houston L.R. (March, 1977): 636 and 639 note.

113. PPSC, Personal Privacy in an Information Society, p. 105.

114. Comment, "Government Access to Bank Records," 14 Houston L.R. (March, 1977): 636.

115. Note (Catherine Carl Wakelyn), "Bank Recordkeeping and the Customer's Expectation of Confidentiality," 26 Catholic University Law Review (1976): 95-96.

116. Comment, "Government Access to Bank Records," 14 Houston L.R. (March, 1977): 642 note.

117. Note, "Government Access to Bank Records," 83 Yale Law Journal (June, 1974): 1443 note. Justice Marshall discussed the pattern

of informal government access to bank records in his dissenting opinion in California Bankers Association v. Shultz, 94 S. Ct. 1494 (1974) at p. 1534-35.

118. See Comment, "Government Access to Bank Records," 14 Houston L.R. (March, 1977): 646-648.

119. For statements of concern for confidentiality by financial institutions and descriptions of disclosure practices supplied to the Canadian Task Force on Privacy and Computers in the early 1970s, see J.M. Carroll et al., Personal Records: Procedures, Practices, and Problems. A Study for the Privacy and Computer Task Force (Ottawa: Departments of Communications and Justice, 1972), pp. 98-102.

120. Bank of Montreal Policies and Procedures Manual, 35-715-7.

121. See I.F.G. Baxter, The Law of Banking and the Canadian Bank Act, 2nd ed. (Toronto: Carswell Co., 1968), p. 21-2 and John M. Sharp, Credit Reporting and Privacy. The Law in Canada and the U.S.A. (Toronto, 1970), p. 65.

122. PPSC, Personal Privacy in an Information Society, p. 49.

123. The question of whether these should be controlled by the Ontario Consumer Reporting Act will be discussed below.

124. John M. Sharp, Credit Reporting and Privacy. The Law in Canada and the U.S.A. (Toronto, 1970), p. 67.

125. Tournier v. National Provincial and Union Bank of England (1924) 1 K.B. 461 (C.A.).

126. Bank of Montreal Form 507, revised 5/74.

127. This working paper treats security primarily from the perspective of protecting the confidentiality of data.

128. For a discussion of the current state of computer crimes or electronic fraud, see August Bequai, "A Survey of Fraud and Privacy Obstacles to the Development of an Electronic Funds Transfer System" 25 Catholic University Law Review (1976): 771-778 and Thomas Whiteside, "Annals of Crime: Dead Souls in the Computer," The New Yorker (August 22, 1977),

pp. 35 ff., and Ibid., (August 29, 1977), pp. 34 ff.; Donn B. Parker, Crime by Computer (New York, 1976) and J.M. Carroll, Computer Security (Los Angeles, 1977).

129. Alan F. Westin and Michael A. Baker, Databanks in a Free Society (New York, 1972), pp. 125-126.

130. Stephen M. Ege, "Electronic Funds Transfer: A Survey of Problems and Prospects in 1975," 35 Maryland Law Review (1975): 42.

131. IBM, Data Security and Data Processing Vol. 1, Data Security Site Publications, GBOF - 1200, pp. 7-8.

132. Alan F. Westin and Michael A. Baker, Databanks in a Free Society (New York, 1972), p. 126.

133. NCEFT, EFT in the U.S., p. 185.

134. Ibid.

135. PPSC, Personal Privacy in an Information Society, p. 114 note.

136. Stephan Kogitz, "Privacy and Data Security: The DP Manager's Viewpoint," Canadian Datasystems (March, 1978), p. 36.

137. Graham Davies, "Computer Fraud. The Crime Companies Won't Report," Financial Times of Canada (November 21-27, 1977), p. 4.

138. Computer Data, II (October, 1977), No. 10.

139. Ibid.

140. Datamation, Vol. 23, No. 6 (June, 1977), p. 180.

141. This information is derived from advertising for the IBM 3614 and from the IBM 3600 Facts Folder, 6th ed. (February, 1977), p. 20.

142. National Commission on Electronic Fund Transfers, Consumer Issues in EFT, Part I: Testimony Presented to the NCEFT, October 26, 1976 (Washington, D.C., October 1977), pp. 43-54.

143. New York Times (March 26, 1978), pp. 1, 30.

144. Information Hotline, IX (December, 1977), pp. 1, 7-10.

145. Details are from Peter N. Drummond, "S.W.I.F.T. Society for Worldwide Interbank Financial Telecommunication," Paper presented at National Security Conference of Canadian Financial Institutions (Toronto, November 14-16, 1977). (hereinafter cited as see Drummond, "S.W.I.F.T. Society"); and Mitchell, "EFT Technology," pp. 52-56.

146. Bank of Montreal, Annual Report 1977, p. 14.

147. Drummond, "S.W.I.F.T. Society," p. 2.

148. Ibid., pp. 4-5.

149. Roger J. Merritt, "Banks and Banking: Florida Adopts a Duty of Secrecy," 22 U. Fla. L.R. (1970): 485.

150. Arthur W. Rogers, Falconbridge on Banking and Bills of Exchange, 7th ed. (Toronto: Canada Law Book, 1969), p. 291.

151. (1924) 1 K.B. 461 (C.A.).

152. Note, "Government Access to Bank Records," 83 Yale Law Journal (June, 1974): 1439.

153. Roger J. Merritt, "Banks and Banking: Florida Adopts a Duty of Secrecy," 2 U. Fla. L.R. (1970): 483 and John M. Sharp, Credit Reporting and Privacy. The Law in Canada and the U.S.A. (Toronto, 1970), pp. 62-70.

154. Haughton v. Haughton, [1965] 1 O.R. 481 at 482.

155. Canadian Encyclopedic Digest, Vol. II 3rd ed. Banking, Title 14 (Toronto: Carswell Co., 1974) p. 14. 54, Sect. 87.

156. John M. Sharp, Credit Reporting and Privacy: The Law in Canada and the U.S.A. (Toronto, 1970), p. 67-68.

157. See Maurice Megrah and F.R. Ryder, Paget's Law of Banking, 8th ed. (London: Butterworths, 1972) pp. 166-186, and I.F.G. Baxter, The Law of Banking and the Canadian Bank Act, 2nd ed. (Toronto: Carswell Co., 1968), pp. 21-24.

158. Diplock L.J. in Parry-Jones v. Law Society, [1968] 1 All E.R. 177, at p. 180.

159. Maurice Megrah and F.R. Ryder, Paget's Law of Banking, 8th ed. (London: Butterworths, 1972), pp. 172-173.

160. S.O., 1976, c. 62, s. 75 (1).

161. S.O., 1976, c. 62, s. 75 (3).

162. R.S.C., 1970, c. E-10, s. 29 (5).

163. R.S.C., 1970, c. E-10, s. 29 (6).

164. R.S.O., 1970, c. 151, s. 34 (4).

165. R.S.O., 1970, c. 151, s. 34 (5).

166. S.O., 1973, c. 97, s. 8 (1).

167. S.O., 1973, c. 97, s. 8 (2).

168. S.O., 1973, c. 97, s. 9 (3).

169. S.O., 1973, c. 97, s. 10 (5).

170. Peterson v. Idaho First National Bank, 367 P. 2d 284 (1961).

171. Ibid., p. 290.

172. Milohnich v. First National Bank, 224 So. 2d 759 (1969).

173. Roger J. Merritt, "Banks and Banking: Florida Adopts a Duty of Secrecy," 2 U. Fla. L.R. (1970): 486.

174. Milohnich v. First National Bank, 224 So. 2d 759 at p. 761. The bank's duty of confidentiality has also been recognized in Iowa and Minnesota. See First National Bank in Lenox v. Brown, 181 N.W. 2d 178 (Iowa, 1970) and Richfield Bank and Trust Company v. Syogren, 244 N.W. 2d 648 (Minnesota, 1976).

175. Bank Secrecy Act of 1970, 12 U.S.C. Secs. 1829 b, 1951-59.

176. From the House of Representatives Report as cited in Comment, "Government Access to Bank Records," 14 Houston L.R. (March, 1977): 637 note.

177. See, for example, Alan F. Westin and Michael A. Baker, Databanks in a Free Society (New York, 1972), pp. 124-125.

178. 94 S. Ct. 1494 (1974).

179. Ibid., at p. 1513. For a discussion of the development of the constitutional right of privacy in the United States in the context of the privacy of bank records see Note, (Francis X. Pray), "A Bank Customer Has No Reasonable Expectation of Privacy of Bank Records: U.S. v. Miller," 14 San Diego L.R. (1977): 416-423.

180. 94 S. Ct. 1494 (1974) at p. 1526.

181. Ibid., p. 1526-1527.

182. NCEFT, EFT in the U.S., p. 24.

183. Comment, "Government Access to Bank Records," 14 Houston L.R. (March, 1977): 648.

184. 96 S. Ct. 1619 (1976), at 1624.

185. Ibid., p. 1624.

186. Ibid., p. 1623.

187. Ibid., p. 1627.

188. Note, (Carol Stein Boyk), "Is There a Right of Privacy in Bank Records? Different Answers to the Same Question: California v. Federal Law," 10 Loyola U.L.R. (March, 1977): 391.

189. Ibid., p. 393.

190. See Comment, "Government Access to Bank Records," 14 Houston L.R. (March, 1977): 637 note.

191. See the remarks made by Robert E. Smith in Business Lawyer, "Electronic Funds Transfer: A Program by the Committee on the Year 2000," Vol. 32 (1976), p. 239.

192. See generally Note (Peter J. Shurn) "Electronic Funds Transfer Systems: A Need for New Law?" 12 New England Law Review (1976): 123-131.

193. NCEFT, EFT and the Public Interest, p. 16.

194. See Comment, "Government Access to Bank Records," 14 Houston L.R. (March, 1977): 638, 651-662.

195. See Computer World, XI, No. 31 (August 1, 1977), pp. 10-11.

196. Daniel A. Fried, "Banking Law. Electronic Funds Transfer." 1976 Annual Survey of American Law, pp. 36-39 and Daniel Prives, "Electronic Fund Transfer Systems and State Laws," 93 Banking Law Journal Vol. 93 (1976): 527.

197. Daniel Prives, "Electronic Fund Transfer Systems and State Laws," 93 Banking Law Journal Vol. 93 (1976): 574-575.

198. Ibid., p. 574-575.

199. Ibid., p. 527.

200. Daniel A. Fried, "Banking Law. Electronic Funds Transfer," 1976 Annual Survey of American Law, p. 39.

201. Daniel Prives, "Electronic Fund Transfer Systems and State Laws," 93 Banking Law Journal Vol. 93 (1976): 572.

202. Flor. Stat. s. 659.062 (10) (1975).

203. Flor. Stat. s. 659.062 (11) (1975).

204. Flor. Stat. s. 659.062 (12c) (1975).

205. Flor. Stat. s. 659.062 (13a) (1975).

206. Flor. Stat. s. 659.062 (13c) (1975).

207. Flor. Stat. s. 659.062 (13d,e) (1975).

208. Burrows v. Superior Court, 529 P. 2nd 590 (1974).

209. Note, (Carol Stein Boyk), "Is There a Right of Privacy in Bank Records? Different Answers to the Same Question: California v. Federal Law," 10 Loyola Law Review (March, 1977): 395-396.

210. 529 P. 2d 590 (1974), p. 593.

211. Ibid., p. 596.

212. Valley Bank v. Superior Court, 542 P. 2d 977 (1975).

213. Ibid., p. 980.

214. People v. Johnson, 53 Cal. App. 3d 394; see also People v. Superior Court, 55 Cal. App. 3d 759.

215. David L. Bazelon, "Probing Privacy," 12 Gonzaga Law Review (1977): 609.

216. Note (Carol Stein Boyk), "Is There a Right of Privacy in Bank Records? Different Answers to the Same Question: California v. Federal Law," 10 Loyola Law Review (March, 1977): 382, 402-407.

217. West's Annotated California Code, Sect. 7461.

218. Ibid., Sect. 7565 b.

219. Ibid., Sect. 7470 a.

220. Ibid., Sect. 7470 c.

221. Ibid., Sect. 7473-76.

222. Privacy Protection Study Commission, Privacy Law in the States (Washington, D.C., 1977), pp. 12-13.

223. Alan F. Westin, Computers, Health Records, and Citizens Rights (Washington, D.C., December, 1976), pp. 275-303.

224. The PPSC found no evidence that depositing institutions collect items of information which could be considered excessively intrusive.

225. Alan F. Westin and Michael A. Baker, Databanks in a Free Society (New York, 1972), pp. 269-279.

226. This issue is discussed in Edward J. Grenier, Jr., "Computers and Privacy: A Proposal for Self-Regulation," 1970 Duke L.J.: 498, 505-509.

227. Lance J. Hoffman, Modern Methods for Computer Security and Privacy (Englewood Cliffs, N.J., 1977), pp. 180-181.

228. Information Hotline, IX (October, 1977), pp. 9-11.

229. Graham Davies, "Computer Fraud. The Crime Companies Won't Report," Financial Times of Canada (November 21-27, 1977), p. 5.

230. NCEFT, EFT and the Public Interest, p. 7.

231. See the discussion in Edward J. Grenier, Jr., "Computers and Privacy: A Proposal for Self-Regulation," 1970 Duke L.J.: 501-502.

232. IBM, COFIS, General Information Manual, 1st ed. (August, 1975), p. 12.

233. Sanford Rose, "Checkless Banking is Bound to Come," Fortune (June, 1977): 120.

234. Computer Data, II, No. 10 (October, 1977).

235. Datamation, XXIII (June, 1977), p. 180.

236. PPSC, Personal Privacy in an Information Society, p. 47.

237. J.M. Sharp, Regulatory Models. A Study for the Privacy and Computer Task (1972), p. 37.

238. Ibid., pp. 38-41.

239. Ibid., p. 36.

240. S.J. Usprich, The Theory and Practice of Self-Regulation. A Study for the Privacy and Computers Task Force (Ottawa, 1972), p. 46.

241. Ibid., p. 40.

242. Ibid., p. 44.

243. Information Hotline, X, No. 2 (February, 1978), pp. 1, 12-14.

244. Computerworld, XI, No. 44 (October 31, 1977), p. 13.

245. PSI Newsletter, X, No. 4 (April, 1978), p. 8.

246. NCEFT, EFT in the U.S., pp. 184-186.

247. Ibid., p. 183.

248. IBM, Data Security and Data Processing Vol. 1, Data Security Site Publishing, GBOF - 1200, p. 7.

249. NCEFT, EFT in the U.S., pp. 260-262.

250. Ibid., pp. 191-192.

251. Ibid., pp. 184, 189-190.

252. See Note, (Peter J. Shurn), "Electronic Funds Transfer Systems: A Need for New Law?" 12 New England Law Review (1976): 122.

253. Alan F. Westin and Michael A. Baker, Databanks in a Free Society (New York, 1972), pp. 238-240.

254. Ibid., p. 279.

255. For a review of non-technical aspects of computer security, including risk analysis, physical security, and administrative methods, see Lance J. Hoffman, Modern Methods for Computer Security and Privacy (Englewood Cliffs, N.J., 1977) pp. 163-183.

256. Lance J. Hoffman, Modern Methods for Computer Security and Privacy (Englewood Cliffs, N.J., 1977) and John M. Carroll, Computer Security (Los Angeles, 1977).

257. IBM, Data Security and Data Processing, Vol. 1, Data Security Site Publishing, GBOF - 1200, p. 10-12.

258. For a review of security features of IBM products see IBM, Data Security Through Cryptography, GC22-9062-0 (1977), pp. 24-28.

259. Thomas Whiteside, "Annals of Crime: Dead Souls in the Computer," The New Yorker (August 29, 1977), p. 58.

260. NCEFT, EFT in the U.S., pp. 188, 191.

261. IBM, Data Security Through Cryptography, GC22-9062-0 (1977).

262. Note, (Peter J. Shurn), "Electronic Funds Transfer Systems: A Need for New Law?" 12 New England Law Review (1976): 123 and NCEFT, EFT in the U.S., p. 191.

263. For a technical description of the Federal Encryption Standard, see Lance J. Hoffman, Modern Methods for Computer Security and Privacy (Englewood Cliffs, N.J., 1977), pp. 78-79.

264. Gina Bari Kolata, "Computer Encryption and the National Security Agency," Science Vol. 197 (July 29, 1977): 438-440 and ibid., Vol. 197 (September 30, 1977): 1345-1349 and New York Times (April 13, 1978), p. 88.

265. NCEFT, EFT in the U.S., p. 57 note.

266. Silver Donald Cameron, "The Death of Money," Quest (November, 1977), p. 32.

267. At a general level, see Robert C. Goldstein, The Cost of Privacy (Brighton, Mass., 1975).

268. Alan F. Westin and Michael A. Baker, Databanks in a Free Society (New York, 1972), p. 315.

269. NCEFT, EFT in the U.S., p. 15.

270. F.E. Balderston, et al., "Computers in Banking and Marketing," Science Vol. 195 No. 4283 (March 18, 1977), p. 1118.

271. 12 U.S.C. 1881-84, (1970); see also Stephen M. Ege, "Electronic Funds Transfer: A Survey of Problems and Prospects in 1975," 35 Maryland Law Review (1975): 39-41.

272. Information Hotline (October, 1977), pp. 1, 7-8; NCEFT, EFT in the U.S. pp. 193-194.

273. The text of the bill is available in Information Hotline (October, 1977), p. 8.

274. Comment, "Government Access to Bank Records," 14 Houston L.R. (March, 1977): 667.

275. (Privacy Report) "Electronic Funds Transfer Systems," The Privacy Report V, No. 3 (October, 1977), p. 7.

276. See for example Note, (Peter J. Shurn), "Electronic Funds Transfer Systems: A Need for New Law?" 12 New England Law Review (1976): 132-134 and PPSC, Personal Privacy in an Information Society, pp. 74, 85, 113.

277. NCEFT, EFT in the U.S., p. 6.

278. Ibid., pp. 5, 307.

279. Ibid., p. 4.

280. Ibid., pp. XV, 7-8, 24-26.

281. NCEFT, EFT and the Public Interest, p. 8.

282. Ibid., p. 29.

283. H. Allan Leal, "Privacy and the Computer," Computers and the Law: Conference Proceedings (Queen's University, 1968), pp. 203-204.

284. Gordon Kaiser, "Constitutional Aspects of the Regulation of Canadian Computer Technology," Queen's Law Journal (1971): 125.

285. Peter T. Burns, "The Law and Privacy: The Canadian Experience," 54 Canadian Bar Review (March, 1976): 48.

286. Canada,Towards an Electronic Payments System, 1975.

287. J.M. Sharp, Regulatory Models, A Study for the Privacy and Computer Task Force (1972), pp. 1-48.

288. Ibid., p. 3.

289. Ibid., pp. 16-29.

290. Ibid., p. 5.

291. See Mitchell, "EFT Technology," pp. 42-43.

292. Ibid., pp. 46-47.

293. Gordon Kaiser, "Constitutional Aspects of the Regulation of Canadian Computer Technology," 1 Queen's Law Journal (1971): 124.

294. Bank Act, S.C., 1890, 53 Vict., C.31, S.46; Bank Act, S.C., 1871, 34 Vict., C.5, S.37.

295. Borrowers and Depositors Protection Act, Bill C-16, 2nd Sess., 30th Parl., 25 Eliz. II, 1976, S. 38 (3).

296. See Loan and Trust Corporations Act, R.S.O. 1970, C.254, SS. 83 (3), 86 (8f), and 178 (1d) .

297. Credit Unions and Caisses Populaires Act, S.O., 1976, C.62, S.145 (e) (f) (g).

298. Consumer Protection Act, R.S.O., 1970, C.82, S.46 (2).

299. See Mitchell, "EFT Technology," pp. 42-43.

300. Telephone Act, R.S.O., 1970, C.457, S.112. This provision has been interpreted as protecting the privacy of telephone conversations: R. v. Chapman and Grange, [1973] 2 O.R. 290.

301. PPSC, Personal Privacy in an Information Society, p. 123.

302. Ibid., p. 122.

303. NCEFT, EFT in the U.S., pp. 37-39.

304. PPSC, Personal Privacy in an Information Society, p. 121.

305. NCEFT, EFT in the U.S., p. 23 note.

306. Ibid., p. 43.

307. PPSC, Personal Privacy in an Information Society, p. 113.

308. NCEFT, EFT and the Public Interest, p. XV.

309. See generally the discussion in NCEFT, EFT in the U.S., pp. 26-35.

310. See the remarks made by Robert E. Smith in Business Lawyer, "Electronic Funds Transfer: A Program by the Committee on the Year 2000," Vol. 32 (1976), p. 239.

311. National Commission on Electronic Fund Transfers, Consumer Issues in EFT, Part I (Washington, D.C., 1976), pp. 20, 41d and (Privacy Report), "Electronic Funds Transfer Systems," The Privacy Report V, No. 3 (October, 1977), p.7.

312. Privacy Protection Study Commission, Privacy Law in the States (Washington, D.C., 1977), p. 27.

313. Note, "Government Access to Bank Records," 83 Yale Law Journal (June, 1974): 1450-1451.

314. Ibid., p. 1455 note.

315. Ibid., p. 1443.

316. Peter T. Burns, "The Law and Privacy: The Canadian Experience," 54 Canadian Bar Review (March, 1976): 24.

317. S.C. 1976-1977, c.33, s.26.

318. Ibid., s.52.

319. Ibid., s.49.

320. Ibid., s.51(1), s.52(2).

321. Peter T. Burns, "The Law and Privacy: The Canadian Experience," 54 Canadian Bar Review (March, 1976).

322. S.B.C., 1968, s.2(1).

323. S.S. 1974, c.80, s.2.

324. S.M., 1970, c.74, s.2.

325. J.M. Sharp, Regulatory Models, A Study for Privacy and Computer Task Force, 1972, p. 4.

326. See Gordon Kaiser, "Constitutional Aspects of the Regulation of Canadian Computer Technology," 1 Queen's Law Journal (1971): 121-125.

327. Newsletter, Commission on Freedom of Information and Individual Privacy (April, 1978), p. 2.

328. Md. Ann. Code, Art. 11, Sects. 224-27, Supp. 1977; Illinois Rev. Stat., ch. 16 1/2, s. 48.1 (Supp. 1977).

329. Note (Catherine Carl Wakelyn), "Bank Recordkeeping and the Customer's Expectation of Confidentiality," 26 Catholic Law Review (1976): 102-105.

330. Ibid.

331. NCEFT, EFT in the U.S., pp. 7-8, 24-26.

332. Ibid., p. 259.

333. This statute is discussed in Phillip J. Scaletta, "Privacy Rights and Electronic Funds Transfer Systems - An Overview," 25 Catholic Law Review (1976): 805 and August Bequai, "A Survey of Fraud and Privacy Obstacles to the Development of an Electronic Funds Transfer System," 25 Catholic Law Review (1976): 789-790.

334. This discussion is based on Comment, "Government Access to Bank Records," 14 Houston L.R. (March, 1977): 667-70.

335. Ibid., pp. 669-70.

336. Information Hotline (October, 1977), pp. 1, 7-8.

337. See Computerworld , XI, No. 46 (November 14, 1977), pp. 1,6.

338. PSI Newsletter (October 1, 1977), pp. 6-7.

339. 95th Cong., 1st Sess., Sect. 2065, introduced September 7, 1977.

340. Ibid., Sect. 802b.

341. Ibid., Sect. 805a.

342. Ibid., Sect. 816.

343. NCEFT, EFT and the Public Interest, pp. 17-18.

344. Ibid., p. 18.

345. Ibid., p. 68.

346. Computerworld , X, No. 37 (September 13, 1976), p. 25.

347. Daniel A. Fried, "Banking Law Electronic Funds Transfer," 1976 Annual Survey of American Law: 39 and Flor. Stat. s.659.062 (13a) (1975).

348. Comment, "Government Access to Bank Records," 14 Houston L.R. (March, 1977): 670.

349. 95th Cong., 1st Sess., Sect. 819.

350. Ibid., Sect. 818.

351. Note (Catherine Carl Wakelyn), "Bank Recordkeeping and the Customer's Expectation of Confidentiality," 26 Catholic U.L. Rev. (1976): 93-94, John M. Sharp, Credit Reporting and Privacy. The Law in Canada and the U.S.A. (Toronto, 1970), p. 68, and Maurice Megrah and F.R. Ryder, Paget's Law of Banking, 8th ed. (London: Butterworths, 1972), p. 166.

352. John M. Sharp, Regulatory Models, A Study for the Privacy and Computer Task Force (1972), p. 5.

353. Ibid., pp. 66-67.

354. Ibid., p. 48.

355. Ibid., pp. 59, 62.

BIBLIOGRAPHY

Abe, Yuzurn. "A Japanese On-Line Banking System." Datamation (September, 1977): 89-97.

Advisory Committee on Automated Personal Data Systems. Records, Computers, and the Rights of Citizens. Washington, D.C., 1973.

Armer, Paul. "Computer Technology and Surveillance." Computers and People Vol. 24, No. 8.

--------. "Electronic Funds Transfer Systems and the Consumer." Computers and People Vol. 25, (June, 1976): 8, 9, 19.

Balderston, F.E., Carman, James M., and Hoggat, Austin C. "Computers in Banking and Marketing." Science Vol. 195, No. 4283 (March 18, 1977): 1115-1119.

Baxter, W.P.C. and Scott, K.E. Retail Banking in the Electronic Age: The Law and Economics of Electronic Funds Transfer. Montclair, N.J.: Allanheld Osmun, 1977.

Bennion, F.A.R. Professional Ethics. London, 1969.

Bequai, August. "A Survey of Fraud and Privacy Obstacles to the Development of an Electronic Funds Transfer System." 25 Catholic University Law Review (1976): 766.

--------. "The Cashless Society: An Analysis of the Threat of Crime and the Invasion of Privacy." 3 Journal of Contemporary Law (1976): p. 47-60.

Binhammer, H.H. Innovation and Change: Deposit Taking Institutions. Economic Council of Canada, 1976.

Brace, Paul. "Electronic Funds Transfer System: Legal Perspectives." 14 Osgoode Hall Law Journal (December, 1976): 787-795.

Brandell, Roland E. "Electronic Funds Transfer: Commercial and Consumer Law Aspects." 82 Commercial Law Journal (March, 1977): 78-85.

--------, and Gresham, Zane O. "Electronic Funds Transfer: The Role of the Federal Government." 25 Catholic University Law Review (1976): 705.

Burns, Peter T. "The Law and Privacy: The Canadian Experience." 54 Canadian Bar Review (March, 1976): 1-64.

California Bankers Association v. Shultz, 416 U.S. 21 (1974).

California Right to Financial Privacy Act, September 28, 1976.

Cameron, Silver Donald. "The Death of Money." Quest (November, 1977): 25-33.

Canada. Towards an Electronic Payments System, 1975.

Canada, White Paper on the Revision of Canadian Banking Legislation. Minister of Finance, August, 1976.

Carroll, John M. Computer Security. Los Angeles, 1977.

--------., Baudot, J., Kirsh, C., and Williams, J. Ivan. Personal Records: Procedures, Practices, and Problems. A Study for the Privacy and Computer Task Force. Ottawa: Depts. of Communications and Justice, 1972.

Comment, (Elaine Block Davis). "Government Access to Bank Records in the Aftermath of U.S. v. Miller and the Tax Reform Act of 1976." 14 Houston Law Review (March, 1977): 636-671.

Committee on the Year 2000. "Electronic Funds Transfer. A Program Presented by the Committee on the Year 2000. Washington, April 10, 1976." 32 Business Lawyer No. 1 (November, 1976).

Courtney, Robert H., Jr. Security Risk Assessment in Electronic Data Processing Systems. IBM: Poughkeepsie, N.Y., May, 1975.

Davies, Graham, "Computer Fraud. The Crime Companies Won't Report." Financial Times of Canada (November 21-27, 1977): 1, 4, 5.

Drummond, Peter N. "S.W.I.F.T. Society of Worldwide Interbank Financial Telecommunication." Paper presented at National Security Conference of Canadian Financial Institutions, November 14-16, 1977, Toronto.

Eddy, H.R. The Canadian Payment Systems and the Computer: Issues for Law Reform, Study Paper. Administrative Law Project of the Law Reform Commission of Canada, 1974.

Ege, Stephen M. "Electronic Funds Transfer: A Survey of Problems and Prospects in 1975." 35 Maryland Law Review (1975): 1-56.

Flaherty, David H. Privacy and Government Databanks. An International Perspective. New York: Science Associates/International, Inc., forthcoming.

Fridman, G.H.L. "Punitive Damages in Tort." 48 Canadian Bar Review (1970).

Fried, Daniel A. "Banking Law. Electronic Funds Transfer." 1976 Annual Survey of American Law: 23-40.

Gellman, Harvey Saul. Electronic Banking Systems and Their Effects on Privacy. A Study by the Privacy and Computer Task Force, Ottawa: Depts. of Communications and Justice, 1972.

Gibson, R. Dale and Sharp, John M. Privacy and Commercial Reporting Agencies. Winnipeg, 1968.

Goldstein, Robert C. The Cost of Privacy. Brighton, Mass., 1975.

Gotlieb, C.C. and Hume, J.N.P. Systems Capacity for Data Security. A Study by the Privacy and Computer Task Force. Ottawa: Departments of Communications, 1972.

Grenier, Edward J., Jr. "Computers and Privacy: A Proposal for Self-Regulation." 1970 Duke Law Journal: 495-513.

Heller, Christopher. "EFT and the Prospects for Individual Privacy." Datamation 21 (September, 1975): 174-178.

Hoffman, Lance J. Modern Methods for Computer Security and Privacy. Englewood Cliffs, N.J., 1977.

I.B.M. Considerations of Physical Security in a Computer Environment. G520-2700-0, 1972.

--------. Data Security and Data Processing 6 Vols. Data Security Site Publications. GBOF-1200.

--------. Data Security Controls and Procedures - A Philosophy for DP Installations. G320-5649-1, 1977 (2nd ed.).

--------. Data Security Through Cryptography. GC22-9062-0, 1977.

--------. Management Memorandum: Security Features of I.B.M. System/370. G320-5650-1, 1977.

--------. Forty-two Suggestions for Improving Security in Data Processing Operations. G520-2797-0, 1973.

Jordan, F.J.E. Privacy, Computer Data Banks, Communications, and the Constitution. A Study for the Privacy and Computer Task Force. Ottawa: Departments of Communication and Department of Justice, 1972.

Kaiser, Gordon. "Constitutional Aspects of the Regulation of Canadian Computer Technology." 1 Queen's Law Journal (1971): 99-126.

Kalven, Harry, Jr. "The Problems of Privacy in the Year 2000," in Daniel Bell, ed., Toward the Year 2000. Work in Progress. Boston, 1968: 244-250.

Kogitz, Stephan. "Privacy and Data Security. The DP Manager's Viewpoint." Canadian Datasystems (March, 1978): 36-40.

Kolata, Gina Bari. "Computer Encryption and the National Security Agency," Science Vol. 197 (July 29, 1977): 438-440.

--------. "Cryptography: On the Brink of a Revolution?" Science Vol. 197 (August 19, 1977): 747-748.

Law Reform Commission of Canada. The Canadian Payment System and the Computer: Issues for Law Reform by Howard R. Eddy. Ottawa, 1974.

Le Valley, James K. and Lancy, John S. "The IRS Summons and the Duty of Confidentiality: A Hobson's Choice for Bankers." 89 Banking Law Journal (1972): 979-997.

Manning, Morris. The Protection of Privacy Act, Bill C-176. An Analysis and Commentary. Toronto, 1974.

Marshall, Geoffrey. "The Right to Privacy: A Skeptical View." 21 McGill Law Journal: 242-254.

Merritt, Roger J. "Banks and Banking: Florida Adopts a Duty of Secrecy." 22 University of Florida Law Review (1970): 482-486.

Mitchell, S. Paula. "Electronic Funds Transfer Technology. A Canadian Perspective. Working Paper #4" December 22, 1977.

Mortimer, Harold E. "The IRS Summons and the Duty of Confidentiality: A Hobson's Choice for Bankers - Revisited," 92 Banking Law Journal (1975): 832-846.

National Commission on Electronic Fund Transfers. EFT in the United States. Policy Recommendations and the Public Interest. Final Report. Washington, D.C., October 28, 1977.

National Commission on Electronic Fund Transfers. Consumer Issues in EFT, Part I: Testimony Presented to NCEFT, October 26, 1976. U.S. Department of Commerce, NTIS, October, 1977.

Note (Francis X. Pray). "A Bank Customer Has No Reasonable Expectation of Privacy of Bank Records: U.S. v. Miller" 14 San Diego Law Review (1977): 414-434.

Note (Catherine Carl Wakelyn). "Bank Recordkeeping and the Customer's Expectation of Confidentiality." 26 Catholic University Law Review (1976): 89-110.

Note (Peter J. Shurn). "Electronic Funds Transfer Systems: A Need for New Law?" 12 New England Law Review (1976): 111-134.

Note "Government Access to Bank Records." 83 Yale Law Journal (June, 1974): 1439-1474.

Note (Carol Stein Boyk). "Is There a Right of Privacy in Bank Records? Different Answers to the Same Question: California v. Federal Law." 10 Loyola University Law Review (March, 1977): 378-408.

Note (Susan M. Knight), "Constitutional Criminal Procedure - Search and Seizure of Bank Records Under the Bank Secrecy Act," 51 Tulane Law Review (1977): 723-730.

Note (Nancy J. Nicol). "No Expectation of Privacy in Bank Records: U.S. v. Miller" 26 DePaul Law Review (Fall 1976): 146-157.

Note (Patrick L. Moore). "U.S. v. Miller: Without a Right to Informational Privacy Who Will Watch the Watchers?" 10 John Marshall Journal of Practice and Procedure (1977): 629-650.

Parker, Donn B. Crime by Computer. New York. 1976.

Payments System Research Program (PSRP). Consumerism and EFTS, May, 1976. Payment Systems, Inc., Atlanta, Georgia.

Privacy Protection Study Commission. Personal Privacy in an Information Society. Washington, D.C. July, 1977.

--------. Privacy Law in the States. Washington, D.C. 1977.

--------. Technology and Privacy. Washington, D.C. July, 1977.

(Privacy Report). "Electronic Funds Transfer Systems." The Privacy Report, V, No. 3 (October, 1977): 1-7.

--------. "Financial Records." The Privacy Report, IV, No. 3 (October, 1977): 1-7.

Prives, Daniel. "Electronic Fund Transfer Systems and State Laws." 93 Banking Law Journal (1976): 527.

Rogers, Arthur W. Falconbridge on Banking and Bills of Exchange. 7th ed. Toronto: Canada Law Book, 1969.

Rose, Peter S. "The Growing Problem of Bank Security." 84 Canadian Banker No. 5 (September - October, 1977): 24-29.

Rule, James B. Private Lives and Public Surveillance. London, 1973.

--------. Value Choices in Electronic Funds Transfer Policy. Washington, D.C.: Office of Telecommunications Policy, October, 1975.

Scaletta, Phillip J. "Privacy Rights and Electronic Funds Transfer Systems - An Overview," 25 Catholic University Law Review (1976): 801-811.

Sharp, John M. Credit Reporting and Privacy. The Law In Canada and the U.S.A. Toronto, 1970.

--------. Regulatory Models. A Study for the Privacy and Computer Task Force Ottawa: Depts. of Communications and Justice, 1972.

Shick, Blair C. "Privacy - The Next Big Issue in EFT." 68 Banking (March, 1976): 70-76.

Simon, Leonard S. "Advances in Electronic Funds Transfer." The Banker (October, 1977): 79-85.

SRI (Stanford Research Institute) Systems Auditability and Control Executive Report. Prepared for the Institute for Internal Auditors, Inc., 1977, G320-5791.

Symposium. "Electronic Funds Transfer Systems." 25 Catholic University Law Review, No. 4 (Summer, 1976): 687-842.

Thompson, Seymour F. "The Invasion of Privacy and Electronic Fund Transfer Systems: Spotlight on the Invaders." Computers and People (September, 1976): 12-13, 19.

United States v. Miller 425 U.S. (1976): 435.

Usprich, S.J. The Theory and Practice of Self-Regulation. A Study for the Privacy and Computer Task Force Ottawa: Depts. of Communications and Justice, 1972.

Weber, William R. "A Public Policy Overview of Electronic Funds Transfer Systems." 25 Catholic University Law Review (1976): 687.

Wessel, Milton R. Freedom's Edge: The Computer Threat to Society. Reading, Mass.: Addison-Wesley, 1974.

Westin, Alan F. and Baker, Michael A. Databanks in a Free Society. New York, 1972.

Whiteside, Thomas. "Annals of Crime: Dead Souls in the Computer." The New Yorker, August 22, 1977: 35 ff.